Povijest DoS i DDoS napada

Razumijevanje DoS Napada

DoS je napad koji ima zacrtan drugačiji cilj od većine napada na računala i mreže. Cyber-kriminalci su koncentrirani na provale u računalne sustave, krađu povjerljivih podataka ili modifikaciju sustava tako da obavlja ilegalnu radnju za koju nije predviđen. Oni često kradu podatke s bankovnih računa i kreditnih kartica, izmjenjujuweb stranice kompanijete šire viruse i općenito nepoželjni softver (eng. malware) kroz mrežu. Te zaraze najčešće doprinose stavljanju tuđih računala pod direktnu ili indirektnu kontrolu napadača. Pored navedenih ilegalnih radnji, uskraćivanje usluge se ne čini vrlo nezgodnim događajem u svijetu cyberkriminala, pogotovo kad se uzme u obzir da ti napadi najčešće potraju samo koliko napadač drži napad aktivnim. Kako su Internet i komunikacija sve više integrirani u naš svakodnevni život, to nažalost više nije točno. Svakodnevno obavljamo višestruke transakcije putem Interneta, nerijetko financijske, poslovne, pa i privatne. Blokiranje tih usluga trajno ili privremeno može imati devastirajući efekt na kompanije koje su uskraćene pružanja svoje usluge, kao i na korisnike koji nisu u mogućnosti pristupiti nekom resursu potrebnom u tome trenutku.

Neki od primjera su:

- Nedostupnost velikih pretraživača Interneta i stranica s novostima povlači direktan financijski gubitak, jer su za svoje usluge plaćeni marketingom na svojoj stranici.
- Bezbroj tvrtki koje se oslanjaju da svoje poslovanje i prodaju obavljaju putem najdostupnijeg medija, Interneta, efektivno gube svakim odbijenim korisnikom koji nije mogao pristupiti stranici. Sam gubitak nije teško prebroditi, ali će se kupci teško pridobiti nazad.
- Financijske institucije koje održavaju usluge Internet bankarstva također gube kako financijsku dobit, tako i povjerenje svojih klijenata.

Sve ove individualne mete gube na jednoj ili više razina kada korisnici ne mogu doći do željene usluge. No postoje i kompanije koje temelje svoje usluge na besplatnom modelu, ali o njihovoj mogućnosti da održe tu uslugu ovisi velik dio Interneta kao ljudima prilagođenog šetališta po digitalnoj mreži. Dakako riječ je o DNS (eng. Domain Name System) poslužiteljima, koji svojom hijerarhijskom propagacijom upućuju svaki upit za imenom stranice u internetski preglednik prema adekvatnoj IP adresi. Kako bi nedostupnost ovih poslužitelja mogla dovesti do kolapsa tog šetališta, očita je bitnost istih za sve korisnike Interneta.

Ciljevi i Motivacija

Cilj DoS napada je ometanje i po mogućnosti obustavljanje normalnog rada nekog sustava. Najčešće su privremeni, ali mogu biti i trajni. Ti napadi postižu se slanjem digitalnih poruka poslužitelju meti koji ga trebaju omesti, usporiti, natjerati ga da obavlja beskoristan rad ili u najgorem slučaju srušiti cijeli sustav. Koliko god bili destruktivni u prirodi, DoS napadi su rijetko kada sami sebi motiv. Prvi DoS napadi su bili, kao i drugi oblici računalnih napada, pokazivanje moći i hvalisanje u podzemnoj zajednici (eng. underground community). Dokazivanje da se nešto može napraviti je bio ultimativni cilj, primjerice preuzimanje IRC kanala ili rušenje određene web stranice. Također, često su se okršaji među dvama članovima takvih zajednica rješavali unakrsnim DoS napadima. Drugi česti motivi su politički, primjerice rušenje stranice organizacija koje zagovaraju politiku protiv hakerske zajednice, ili

nekih ideologija i pogleda koje nisu po volji pojedinaca ili grupa. Često se događa i da druge kompanije unajmljuju napadače da obustave rad sustava konkurenata da bi se dobila prednost na tržištu. U skorije vrijeme sve češći su DoS napadi iznuđivanja, gdje se organizacija upozori prije ili tokom napada te se traži određena suma da bi se napad obustavio.

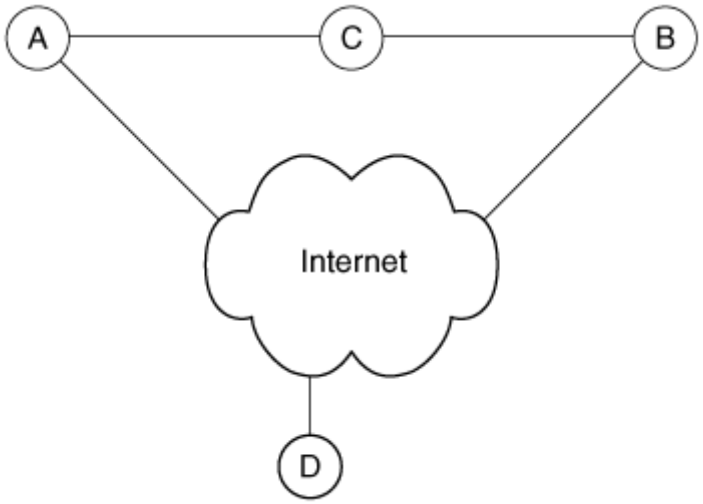
Odnos DoS napada i Interneta

Temeljne ideje koje stoje iza DoS napada proizlaze iz postavki po kojima je građen današnji Internet. Kako se Internet razvio iz ARPANET-a, sustava napravljenog početkom šezdesetih godina prošloga stoljeća na temelju tadašnjih uvjeta povezivanja sustava, i njemu sličnih projekata uzeo je najbolje principe koji su tada postojali.Nažalost sve mane tih principa su temelj na kojem se grade DoS napadi na računalne mreže i sustave, te će neke biti pomnije proučeni u nastavku.

Packet-Switching

Ključna ideja u dizajnu Interneta je packet-switching (paketima upravljano preusmjeravanje). Ona je revolucionalizirala način na koji računala danas komuniciraju. Revolucionarna je u pogledu zamjenecircuit-switchinga , starog oblika povezivanja dvaju korespondenata, novom mrežom jeftinih redundantnih čvorova (end. node) koji su međusobno mogli komunicirati da šalju podatke najkraćim mogućim putem od točke A do točke B. Takvom redundancijom postizala se velika pouzdanost sustava. Pošiljatelji i primatelji su komunicirali preko paketa, gdje je svaki paket sadržavao informaciju o izvorištu i krajnjoj destinaciji, kao i sam podatak koji prenosi. Sama ruta nije bila predefinirana nego je svaki čvor u lancu birao kojemu će dalje poslati da bi informacija što brže stigla do odredišta. U slučaju otkazivanja određenog čvora informacija bi se jednostavno preusmjerila preko drugog para u lancu, odnosno našla bi se alternativna putanja. Ovako dizajnirani sustavi doprinose brzom, efikasnom, jeftinom i vrlo pouzdanom načinu izgradnje sustava mreža. Nažalost te iste odrednice koje pospješuju funkcionalnosti sustava ga ostavljaju izrazito ranjivim. Od kojih su najizraženije:

- Nema dediciranih kanala koji povezuju pošiljatelja i primatelja. Ovo omogućava višestruko povećanje prometa među sustavima, tako što se protok informacija dijeli među vezama. Manjak ovog principa je da nema nikakve garancije da će se određeni resursi alocirati kanalu, te napadači koriste ovu tehniku kako bi preplavili kanal i „izgladnili“ druge korisnike od njihovih resursa. Ovaj problem se regulira dijeljenjem resursa (eng. Resource sharing) između svakog korisnika, tj. njegove IP adrese. Nažalost napadači ovo također zaobilaze lažiranjem više IP adresa ili napadom s više strojeva odjednom.
- Paketi putuju bilo kojom rutom između pošiljatelja i primatelja.Primjenom ovog principa paketi slobodno putuju između središnjih čvorova tako da se odabire najbolji dostupan čvor. Donja slika Prikazuje princip gdje u vezi čvora A i B, čvor D može preuzeti preusmjeravanje paketa među njima ukoliko čvor C nije dostupan. Ukoliko prvi odabran čvor nije dostupan odabire se alternativni pomoću dinamičkih algoritama odabira puta. Stoga nijedan čvor ne zna konačnu putanju paketa od pošiljatelja do primatelja. Upravo ova ideja onemogućava detekciju i filtriranje lažnih IP adresa (eng. IP Spoofing) koje su jedno od glavnih alata pri DDoS napadima.



- Različite veze omogućavaju različitu propusnost. To je logičan princip dizajna mreže koji se nametnuo njenim korištenjem. Danas Internet ima izgled paukove mreže s mnogo krajnjih izdanaka. Shodno takvom razvoju središnji dio je dobro povezan s više redundantnih čvorova i podržava veliku propusnost podataka, dok krajnji dijelovi omogućavaju manju propusnost i povezani su najčešće s par čvorova. Ovakva topologija, makar bila logična, stvara probleme u trenutku kada se velike količine podataka pokušavaju prenijeti iz središta mreže do nekog krajnjeg čvora. Promet iz središta preoptereti vezu na krajnjim čvorovima i to je činjenica na kojoj se zasniva većina DDoS napada.

Best-Effort model i end-to-end paradigma

Krajnji cilj pri izgradnji današnje Internet infrastrukture je pomicanje informacija od točke A do točke B što brže i po što manjoj cijeni. Po toj ideji je nastao Best-Effort model prijenosa podataka (eng. Best-Effort Service Model). Ideja iza toga je da se svi paketi u mreži tretiraju kao jednaki, tj.daje im se jednako „truda“ odnosno rada pri obradi, te se pretpostavlja da će biti obrađeni. Tim postavkama je omogućena izgradnja jeftine mreže gdje se paketi u čvorovima obrađuju brzo i jeftino pomoću usmjerivača (eng. router), koji su jednostavni i specijalizirani strojevi namijenjeni za tu funkciju. Druga postavka kod izgradnje mreža koja se razvila u isto vrijeme kad i packet-switching je end-to-end princip, koji je jedan od centralnih principa izgradnje Interneta. Kako je još u to vrijeme predviđeno da će Internet imati više namjena koji još nisu ni otkrivene,odlučeno je postaviti jednostavnu strukturu mreže. Princip pretpostavlja da sve potrebne postavke za funkcioniranje određene aplikacije, primjerice pouzdana dostava paketa, korekcija grešaka u prijenosu, enkripcije i slično, neće biti implementirane među svim čvorovima koje prenose pakete nego samo između krajnjih točaka prijenosa, pošiljatelja i primatelja. Time je zacrtano da kod implementacije novog protokola ili servisa treba raditi izmjene i dogradnje samo kod krajnjih točaka prijenosa. Tim dvama principima postavljen je jednostavan temelj Interneta koji je izgrađen na jednoj jedinstvenoj ideji: “Središte mreže mora ostati jednostavno, sva kompleksnost izgradnje se treba seliti na rubne točke sustava“. Implementacija tih postavki postignuta je grupom protokola poznatom kao TCP/IP ili Internet Protocol Suite, koja je podržana od svih usmjeritelja i čvorova unutar Interneta. Krajnji čvorovi veze primjenjuju i druge protokole specifične za određene zahtjeve aplikacija, primjerice User Datagram Protocol (UTP) za jednostavan tok podataka, Real Time Protocol (RTP) i slični. Time je omogućeno održanje funkcionalnosti mreže prilikom njene nagle ekspanzije i povećanja prijenosa podataka, a a da je ona pritom jeftina za održavanje. Nažalost ta ista prednost onemogućava implementaciju nadzora i detekciju DDoS napada u samom centru mreže otkuda najčešće i dolaze napadi, nego se to prepušta krajnjim točkama, gdje je jednom kad protok podataka stigne često prekasno za ikakvu efektivnu

obranu. Kod takvih napada zagušivanje mreže je glavni problem koji nastaje najčešće kao posljedica DDoS napada i IP spoofinga. Da bi se djelomično sanirali problemi koji nastaju kod takvog dizajna Interneta prekršen je djelomično end-to-end princip. Primijenjena su dva mehanizma regulacije protoka paketa, točnije aktivno praćenje reda (eng. Active queue management, AQM) i algoritmi poštene obrade (eng. Fair scheduling algorithms) koji su integrirani u današnje usmjernike. Ubuduće će se vjerojatno morati primijeniti slične tehnike za regulaciju DDoS napada unutar središta Interneta.

Evolucija Interneta

Jedan od glavnih razloga uspješnosti DoS napada je i nagli razvoj Interneta. Njegovom ekspanzijom iz globalne znanstvene mreže u globalnu komunikacijsku okosnicu iznjedrili su sigurnosni propusti koji nisu mogli biti predviđeni u ranim fazama razvoja, a nasljedstvo su prijašnjih principa. Ti problemi su:

- Količina povezanih računala, gdje je u početku ARPANET dopuštao maksimalno 64 povezana računala.Danas po statistikama Internet snabdijeva skoro dvije milijarde korisnika informacijama odnosno 30% stanovništva Zemlje. Shodno tom enormnom rastu povećao se i broj strojeva koji su neadekvatno osigurani, te danas napadači imaju velik broj lakih meta koje mogu dodati u svoj botnet , a taj broj konstantno raste.
- Profil korisnika se također dosta promijenio. U prošlosti je prosječan korisnik bio visoko obrazovan znanstvenik pri nekom institutu koji je posjedovao poprilično količinu znanja o računalima i koji je koristio vrlo određene aplikacije za svoje potrebe. Danas glavnu bazu korisnika čine kućni korisnici koji imaju malo ili ništa iskustva s računalnom sigurnosti i koji koriste razni spektar aplikacija, nerijetko i ilegalno dobavljene verzije softvera koje sadrže maliciozan softver zamaskiran u aplikaciju.Takav zlonamjeran softver je poznat kao trojanski konj (eng. Trojan Horse).
- Popularnost Interneta koja je proizašla iz njegove ekspanzije nije došla bez žrtvi.Takav sustav koji je visoko integriran u naše živote postaje meta napada baš zbog te iste popularnosti gdje šteta nastala pri napadu raste razmjerno s popularnošću mete.

Promatranjem svih ovih činjenica, nepobitno je da DoS napadi utječu direktno na naš život te treba shvatiti težinu koju takvi napadi imaju ukoliko su uspješni. Da bi mogli bolje razumjeti kako spriječiti napade i štete proizašle iz njih,u sljedećem poglavlju su obrađene najčešće vrste napada i kako se oni izvode.