SVEUČILIŠTE U ZAGREBU

FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Seminarski rad iz kolegija Računalna forenzika

Mrežni DDoS napadi

Bruna Anđelić, 0036478714

Zagreb, siječanj 2018.

Sadržaj

Uvod

DDoS napadi su distribuirani napadi ostvareni metodom uskraćivanja usluge. Ova vrsta napada prisutna je već dugo te se redovito pojavljuje, ali sa sve većom sofisticiranošću i snagom. U početku je to bila najjednostavnija vrsta mrežnog napada u kojoj se doslovno slanjem *ping* zahtjeva s napadačeva računala pokušavao preplaviti poslužitelja koji je bio žrtva. Ali kako to biva u stalnoj borbi između napadača i stručnjacima za zaštitu i sigurnost, stvari su se od tada znatno promijenile. Sa svakim novim načinom zaštite napadači osmisle novi rigorozniji način napada koji je sve teže detektirati i od njega se obraniti. Sada se oko ove vrste napada razvio unosan posao te je moguće iznajmiti *botove* za izvršavanje distribuiranog napada i to po satu, također postoje mnoge skripte koje su javno dostupne i mnoga već gotova rješenja koja postaju vrlo opasno nađu li se u krivim rukama. Također aplikacijski DDoS napadi su u velikom naletu razvitka te postaju sve sofisticiraniji i teži za detektiranje i rješavanje.

U sljedećim poglavljima ovog seminarskog rada prvo će se čitatelja upoznati općenito s DDoS napadom te razlikom između DoS i DDoS napada zajedno s logistikom samih napada. Nadalje će se napraviti podjela napada u 3 kategorije te će se svaka od kategorija zasebno pobliže objasniti. Budući da je osim poznavanja napada jako bitno znati i koje se mjere opreza mogu koristiti u prevenciji napada ta će se tema također razraditi kroz poglavlje. Na kraju će se izvesti zaključak o svih informacijama predstavljenim kroz seminarski rad.

1. Općenito o mrežnim DDoS napadima

DoS (*eng. Denial-of-Service*) je, kako samo ime govori, napad uskraćivanjem usluge. Ideja iza ove vrste napada je da se pomoću preplavljivanja neka online usluga učini nedostupnom za svoje legitimne korisnike. Distribuirani napad uskraćivanja usluge ili DDoS (*eng. Distributed Denial-of-Service*) razliku je se od DoS napada isključivo po broju računala s internetskom konekcijom koji sudjeluju u napadu. Prilikom DoS napada napadač koristi samo jedno računala s internetskom konekcijom, dok je prilikom DDoS napada korišteno mnoštvo računala. DDoS napad nastaje kada više prethodno kompromitiranih, odnosno zaraženih, računala, koji se zajednički nazivaju *botnet,* preplavljuju resurse sustava koji se želi napasti, a koji se obično sastoji od jednog ili više web poslužitelja. Budući da je za napad prilikom DDoS napada potreban velik broj računala kojima napadač upravlja i pomoću kojih sinkronizirano izvršava napad potrebno je prije samog napada napraviti pripremu koja se sastoji od izgradnje takvog sustava. Budući da vrijeme koje je potrebno uložiti u izgradnju takvog sustava nije zanemarivo postoje mnoge tehnike kojima vješti napadači danas zauzimaju sustave drugih korisnika, a najčešći među njima su trojanski konj i virusi koje napadači propagiraju kroz sustave ili aplikacije s poznatim propustima koje napadači koriste kako bi dobili administrativna prava nad sustavom. Sama uspješnost i jačina napada povećava se kroz povećanje i strukturiranje *botneta*, a jačina napada uvelike ovisi i o brzini mreže žrtve i napadača. Nakon što napadačev *botnet* poprimi dovoljne razmjere on se strukturira kako bi napadač komunicirao samo s manjim brojem računala, nazvanim gospodari, koji zatim kontroliraju napadačke sustave. Tako se napad izvodi jednostavnije, a napadača je teže pronaći preko IP adrese. Jednom kada je sustav strukturiran i spreman za napad jedna naredba napadača je sve što je potrebno kako bi se izvršio napad na zadanu metu. Napadačeva naredba propagira se gospodarima koji dalje adresu prosljeđuju napadačkim sustavima te kreće napad s više strana na zadanu metu. Upravo je ta struktura napadačevog *botneta,* koja osigurava veću uspješnost napada, razlog zašto se DDoS većinom koristi umjesto DoS napada iako je struktura samog napada najčešće jednaka.

2. Podjela DDoS napada

DDoS napadi mogu se podijeliti na više vrsta, a uglavnom se razlikuju po tipu i količini prometa koja10 se koristi prilikom napada te po ranjivosti koja se iskorištava. Unutar ovog seminarskog rada DDoS napade podijelit ćemo na amplifikacijske (masovne), protokolne te aplikacijske napade.

2.1 Amplifikacijski DDoS napadi

Ovo je najčešće korišteni tipa DDoS napada, a u njemu se koristi golema količina prometa. Iako ovaj napad karakterizira velika količina prometa, nekada i preko 100 Gbps, oni ne zahtijevaju da taj promet generiraju sami hakeri. Upravo zbog te činjenice ovaj se tip DDoS napada smatra najjednostavniji za izvođenje. Napadači reflektiraju malu količinu prometa te tako u mreži generiraju velik promet. Napadi ovog tipa koji se baziraju na refleksiji ciljaju sustav koji napadaju slanjem zahtjeva na DNS ili NTP server korištenjem lažirane izvorišne IP adrese. Kada DNS ili NTP server odgovaraju na zahtjev zapravo odgovaraju na odredišnu adresu zahtjeva koja je lažirana. U ovom slučaju lažirana IP adresa je adresa žrtve napada koja zatim bude preplavljena podacima. Ovakav način preplavljivanja zanimljiv je napadačima jer primjerice jedan zahtjev prema DNS-u najčešće rezultira s više odgovora. Pa tako ako se koristi ANY tip zahtjeva promet se može povećati i do 70 puta. Prilikom ovog napada količina prometa koja se generira dovoljna je da potpuno blokira pristup žrtvi.

2.2 Protokolni napadi

Napadači su pri izvođenju ove vrste napada primarno fokusirani na iskorištavanje propusta 3. i 4. sloja OSI referentnog sustava. Najpoznatiji primjer iskorištavanja slabosti 4. sloja je SYN preplavljivanje. Ova vrsta napada koristi transportni protokol TCP. Za uspostavu konekcije TCP protokol koristi postupak trostrukog rukovanja. Klijent pošalje SYN paket na koji poslužitelj odgovara sa SYN ACK na što opet klijent odgovara s ACK paketom. Nakon što je trostruko rukovanje završilo TCP konekcija je uspostavljenja i u ovom trenutku aplikacija počinje slati podatke korištenjem 7. ili aplikacijskog sloja kao što je primjerice slanje HTTP zahtjeva.

Prilikom SYN preplavljivanja poslužitelj se preplavljuje slanjem SYN paketa te zatim ignoriranjem SYN ACK odgovora od strane poslužitelja. Budući da TCP čeka na odgovor klijenta ovim se načinom iskoriste svi resursi TCP poslužitelja samo na čekanje konfiguriranog vremena na primitak ACK poruke koja bi trebala doći od strane klijenta. Budući da su web i aplikacijski poslužitelji ograničeni brojem otvorenih konkurentnih TCP konekcija, ako napadač pošalje dovoljno SYN paketa na poslužitelj on ga lako može blokirati i tako onemogućiti legitimne zahtjeve korisnika sustava upućene prema tom poslužitelju.

2.3 Aplikacijski napad

Aplikacijski su napadi najkompliciranije vrsta DDoS napada te su stoga i teži za detekciju, a u nekim slučajevima i za izbjegavanje i smanjenje utjecaja napada na servere. Napadi aplikacijskog sloja su najsofisticiraniji napadi jer su iznimno efektivni s vrlo malo resursa, primjerice s jednim računalom koje sporo generira promet. Upravo zato ove je napade jako teško proaktivno detektirati s tradicionalnim rješenjima za detekciju i prevenciju napada. Napadači koji izvode ovu vrstu napada su vrlo vješti i imaju duboko znanje o radu aplikacija i protokola, za razliku od primjerice amplifikacijskih napada za koje nije potrebno gotovo nikakvo predznanje napadača. Aplikacijski napadi iskorištavaju propuste 7. sloja OSI referentnog sustava. Najčešće se izvršavaju pomoću HTTP GET funkcije, što znači da je trostruko rukovanje TCP-a izvršeno te da su prevareni svi sustavi koji provjeravaju samo 4. sloj i TCP komunikaciju. Napadač sustavu izgleda kao legitimni korisnik konekcije te mu je dopuštena komunikacija s web sustavom ili aplikacijom. Kada se ova faza izvrši napadač počinje zahtijevati veliku količinu datoteka ili objekata korištenjem HTTP GET funkcije. Generalno su to ispravni zahtjevi, ali problem je što ih je mnogo. Toliko da poslužitelj brzo postane prezaokupljen odgovaranjem na te zahtjeve pa mu je teško odgovarati na nove zahtjeve legitimnih korisnika. U početku je ovaj napad bio zaustavljen ograničavanjem brzine za korisnika, ali napadači su ovo ograničenje iskoristili kako bi smislili novo rješenje za još teži napad, kako to i inače biva. Prepreku su premostili korištenjem distribuiranog sustava *botova* kako bi se osiguralo da se zahtjevi šalju s različitih IP adresa te je tako napad postao teži i za detektiranje i za zaustavljanje. Osim korištenja *botova* napad se izvršava i kada se dovoljno napadača zajedno udruže kako bi napali stranicu koji ih iz nekog razloga sve smeta.

Ova vrsta napada teža je za detekciju od napada na 4. sloju jer u njemu postoji validna TCP konekcija a i svi zahtjevi koji se šalju su validni. Napad bi se trebao prepoznati kada se primijeti da postoji više klijenata koji zahtijevaju veliku količinu objekata u isto vrijeme. Problem je u tom što to mogu biti i legitimni korisnici koji su pomiješani zajedno s napadačima pa ako svima uskratimo uslugu napadači upravo dobivaju ono što su od početka željeli. Obrana protiv ovog tipa napada je najčešće korištenjem nekog algoritma za formiranje brzine koji promatra sve klijente i osigurava da nitko u određenom vremenskom periodu, najčešće minutama ili sekundama, ne šalje više zahtjeva od onog određenog granicom. Ako korisnik šalje više od ograničenog broja zahtjeva njegova se IP adresa stavlja na crnu listu i onemogućena mu je usluga na tom sustavu u određenom vremenskom periodu, što također još uvijek može utjecati i na legitimne korisnike sustava. Iz tog su razloga postoje još mnoga otvorena pitanju o zaustavljanju i prevenciji ovih napada za čije je odgovore potrebno duboko razumijevanje i znanje o aplikacijskom sloju.

3. Prevencija DDoS napada

Kao što je napomenuto DDoS napadi su jedni od najčešće korištenih vrsta mrežnih napada koji su već neko vrijeme popularni među napadačima. Oni godinama postaju samo sve više sofisticirani i snažniji te ih je sve teže detektirati ili se od njih obraniti. Kako napadači svaki dan smišljaju nove inovativne ideje eksploatacije i napada potrebno je s njima držati korak te otkriti i implementirati metode prevencije i obrane od svake nove vrste napada. U prethodnom poglavlju opisane su neke od osnovnih vrsta ovog tipa napada te je objašnjena složenost i snaga svakog. Kako je vidljivo za najjednostavniji tip napada nije potrebno gotovo nikakvo predznanje o ovom području. Trenutno na Internetu postoji gomila skripti i gotovih rješenja koja su pisana u popularnim programskih jezicima te ih je lako shvatiti i prilagoditi svojim potrebama. Također postoji prilično jako tržište i ako imate dovoljno novca možete osigurati napad katastrofalnih posljedica na odabranu žrtvu. Upravo iz činjenice da je ovo područje u tolikom naletu i tako se razvija i širi munjevitom brzinom potrebno je biti svjestan što se sve može učiniti kao mjera opreza i prevencija protiv svih vrsta ovakvih napada.

Iznimno je bitno unaprijed razmišljati o prevenciji ove vrste napada te iako se ne mogu poduzeti apsolutne mjere prevencije postoje koraci kojim se napadačima otežava izvršenje zloćudnog plana. Za početak bitno je arhitekturu učini što otpornijom što je svakako važno ne samo zbog otpornosti na DDoS i druge vrste napada već i radi osiguravanja konzistentnog izvođenja sustava te time u konačnici i privlačenja i zadržavanja korisnika. Mjere koje se mogu poduzeti po tom pitanju su primjerice lokalizacija poslužitelja u različitim podatkovnim centrima i osigurati da se oni nalaze na različitim mrežama te osigurati da u sustavu ne postoji jedinstvena točka ispada. Kod većih sustava bitno je da se osigura da su resursi koji se koriste geografski raspršeni te da oni nisu lokalizirani na jednom podatkovnom centru. Nadalje danas postoji mnogo hardverskih rješenja koji omogućavaju izbjegavanje ove vrste napada kao što su primjerice vatrozidi koji pomažu zaštiti od napada na 4. sloju. Mnoštvo današnjih gotovih rješenja sadrži postavke koje omogućuju operatoru mreže da počne zatvarati TCP konekcije nakon što je dosegnuta određena granica zasićenja i sl. Također, ako je to moguće, trebalo bi povećati mrežni *bandwidth* koji pomažu prevenciji amplifikacijskih napada. Tako nastaje borba između volumena mrežnih zahtjeva koji sustav može podnijeti i volumenom zahtjeva koji napadač može poslati. Ali budući da je količina zahtjeva koju napadači mogu poslati golema

ovo je rješenje primarno za velike organizacije koje si tako veliki *bandwidth* mogu priuštiti. Nadalje moguć je *outsourcing* zaštite od napada *providerima* specijaliziranim za skaliranje infrastrukture sustava kako bi što bolje odgovarali na pokušaje napada. Oni mogu ukloniti većinu problematičnog prometa i prije no što dođu do mreže žrtve. Ostale mjere opreza ne temelje se toliko na prevenciji koliko na brzom i efektivnom odgovoru na bilo koju od vrsta DDoS napada. Postoje tako i *provideri* koji su specijalizirani za akcije koje je potrebno napraviti tijekom samog DDoS napada. Oni u tim slučajevima preusmjeravaju destinacije žrtvine mreže u centar za ublažavanje efekata napada gdje se sav promet filtrira i samo se promet legitimnih korisnika preusmjerava do poslužitelja koji je žrtva napada. Takvi *provideri* su spremi podnijeti velike količine prometa koji su mogući kao rezultat bilo kojeg tipa DDoS napada.

4. Zaključak

Izvješća pokazuju da se je godišnji porast učestalosti DDoS napada u godini dana porastao ukupno za 4%. Pogledamo li pobliže tu statistiku vidljivo je da se veći porast očituje u složenijim vrstama ovog napada. Tako je primijećen porast u protokolnim napadima u iznosu od 6%, 22% porasta vidljivo je u onima baziranim na refleksiji, dok je porast napada većih od 100 Gbps-a oko 140% [9]. Jedan od najnovijih načina eksploatacije ranjivosti koji danas donosi najveću opasnost je iskorištavanje Interneta stvari (IoT uređaja) kao *botova*. Kao i obično programeri i inženjeri koji razvijaju neku novu tehnologiju ne misle previše o tamnoj strani svojih dostignuća i mogućnosti zlouporabe istih. Tako Internet stvari nije imao nikakve zakonske obveze za bilo kakvim dodatnim sigurnosnim regulacijama. Svaka i najmanja neopreznost na ovom području brzo se otkrije i iskoristi od strane iskusnih napadača pa su se tako nedugo nakon početka intenzivnije uporabe Interneta stvari pojavili *botnetovi* kao što je primjerice Mirai koji uređaje Interneta stvari pretvara u *botove.* Time se otvorila cijela grana novih mogućnosti izvođenja ove vrste napada koje imaju značajne posljedice i smatra se da je čak 7 od 12 napada većih od 100 Gbps-a izravno povezano s Mirai [9]. Za očekivati je da će se u budućnosti kroz razvijanje novijih tehnologija ovaj broj značajno povećavati ako stručnjaci za zaštitu i sigurnost brzo ne uhvate korak s novim tipovima DDoS napada. Iz svih navedenih razloga vidljivo je da je neophodno educirati se i poduzeti sve potrebne mjere opreza za ovakve tipove napada kao što je i neophodno da se sami sustavi zaštite i obrane sve više razvijaju i napreduju.

5. Literatura

[1] https://www.cis.hr/WikiIS/doku.php?id=dos_attacks

[2] https://sucuri.net/website-firewall/ddos-protection

[3] https://www.cloudflare.com/ddos/

[4] https://www.webopedia.com/TERM/D/DDoS_attack.html

[5] https://devcentral.f5.com/articles/layer-4-vs-layer-7-dos-attack

[6] https://blog.thousandeyes.com/three-types-ddos-attacks/

[7]https://www.techrepublic.com/blog/it-security/ddos-attack-methods-and-how-to-prevent-or-mitigate-them/

[8] https://insights.sei.cmu.edu/sei_blog/2016/11/distributed-denial-of-service-attacks-four-best-practices-for-prevention-and-response.html

[9] https://blogs.akamai.com/2017/03/ddos-of-past-present-and-future.html