Analiza pouzdanosti Cloud computing rešenja na DDoS napade

Predrag Alargić, Tanja Kaurin
Fakultet za pravne i poslovne studije dr Lazar Vrkatić
Novi Sad, Srbija
predrag.alargic@useens.net, tanja.kaurin@useens.net

Sadržaj—**Bezbednosni incidenti su sve više prisutni na Internetu, ako uzmemo u obzir ne samo one koji kompromituju krajnje korisnike, već i one koji napadaju velike računarske sisteme, kao što su kompanije sa multinacionalnim poslovanjem, državni organi ali i pružaoci internet usluga. Zlonamerni napadi koji su usmereni ka krajnjim korisnicima skoro uvek dolaze kao maliciozni program koji degradira performanse korisničkih računara i ima sposobnost prikupljanja osetljivih podataka. Napadači skoro uvek preko malicioznog softvera preuzimaju kontrolu nad računarima koji su zaraženi, sa ciljem da izvedu koordinisani napad. Infrastrukturu koju pružaju internet provajderi, državni organi ali i velike kompanije koristi puno korisnika. Krajnji rezultat ovakvih napada je skoro uvek velikih razmera. U ovom radu, uz osvrt na DDoS napade i Cloud computing rešenje kao jedno od rešenja, analiziraćemo pouzdanost Cloud computing rešenja u incidentnim situacijama.**

Ključne reči - DDoS napad; Cloud computing; bezbednosni aspekti

I. UVOD

Poslovni sistemi danas nisu spremni da se zaštite od DDoS napada, četiri od deset poslovnih sistema nemaju čak ni strategiju odbrane od ovakve vrste napada. Nedostatak znanja i zaštite stavlja poslovne sisteme u opasnost od gubitka važnih podataka čak i do zastoja u radu. DDoS napadi (eng. „Distributed Denial of Service“) mogu brzo onesposobiti ciljani poslovni sistem i uticati na tok rada. U praksi se pokazalo da gotovo petina (16%) poslovnih sistema uopšte nisu zaštićeni od DDoS napada, a polovina (49%) se oslanja na opremu koju poseduje, čija je svrha zaštita. U praksi se pokazalo da to nije dovoljno kao rešenje za borbu protiv sve većeg broja velikih napada ali i sve većeg broja „pametnih“ DDoS napada koje je teško otkriti i filtrirati sa standardnim, postojećim metodama.

DoS napadi (eng. Denial-of-service) su u porastu te su se razvili u složenije i skoro pa nesavladive prepreke za male ali i velike poslovne sisteme. Iako DoS napadi nisu novija pojava, metode i resursi koji su na raspolaganju za odbranu od ovakve vrste napada svakim danom se razvijaju kao i alati i postupci a naročito od pojave DDoS napada. U novije vreme učestala je pojava napada korišćenjem distribuiranih reflektora ili drugačije nazvanih DRDoS napada (eng. Distributed Reflection Denial of Service) čije otkrivanje i sprečavanje nije moguće korišćenjem tradicionalnih rešenja i metoda. Danas postoji veliki broj alata čija je uloga efikasna odbrana od DDoS napada u Cloud computing rešenju. Veliki broj alata koji su nam dostupni rade na principu usluga na mrežnom kraju. Mogu se koristiti za ublažavanje DDoS napada svih oblika i veličina, uključujući i one koje su usmerene na UDP i ICMP protokole, kao i SYN / ACK i Layer 7 napade.

Cloud computing rešenje kao sistem kontrole nad podacima, premešta sa klijentske organizacije na cloud provajdere, gotovo na isti način na koji organizacije povere deo svojih IT poslovanja spoljnim preduzećima. Osnovni zadaci, koji se ogledaju u primeni sigurnosnih zakrpa ali i samo podešavanje sigurnosnog, odnosno zaštitnog zida, kao dodatna usluga može postati odgovornost pružaoca Cloud computing usluga, a ne korisnika. Kao rezultat toga, korisnik mora da uspostavi odnos poverenja sa pružaocem Cloud computing usluge i da bude svestan rizika da njegov pružalac izvršava, primenjuje i upravlja bezbednosnim opcijama umesto samog korisnika[1].

Međutim danas, neki veliki poslovni sistemi biraju privatne ili hibridne modele Cloud computing rešenja umesto javnih i to samo zbog rizika koji su u vezi sa spoljnim servisima. Time poslovni sistemi imaju mogućnost brzog reagovanja na DDoS napade. Brzina detektovanja DDoS napada predstavlja bitan činilac u rešavanju probema izazvanih ovakvom vrstom napada. U ovom radu će biti prikazan i analiziran rad nekoliko alata čija je uloga zaštita mrežnih sistema prilikom DDoS napada.

II. CLOUD COMPUTING

Definicija Cloud computing rešenja nije tako jednostavna. Trenutno se izdvaja nekoliko definicija a napomenućemo samo dve. Prva definicija koja se izdvaja je Gartnerova definicija: “To je skup disciplina, tehnologija i poslovnih modela koje se koriste da isporuče IT mogućnosti (softver, platformu i hardver) po zahtevu, da bude skalabilna i elastična usluga” [2].

Druga definicija Cloud computing rešenja, je definicija Američkog Nacionalnog instituta za tehnologiju i standarde

(NIST) koja glasi: “Cloud computing je model koji omogućava jedinstven, precizan pristup deljivim računarskim resursima koji mogu da se konfigurišu (mreže, serveri, skladišta podataka, aplikacije i usluge) i mogu na zahtev, brzo da se realizuju uz minimalne resurse i uz minimalnu interakciju sa pružaocima usluga” [3].

Razlika između tradicionalnog pristupa računarstvu i Cloud computing rešenja je da se u tradicionalnom pristupu podrazumeva kupovina programa i smeštanje istog na računarski sistem, bio on u vidu radnih stanica ili personalnih računara, dok u Cloud computing rešenjima poslovni sistem najčešće plaća samo naknadu za korišćenje. Možemo reći da kupovina kompletnog računarskog sistema i rešenja koja se smatra tradicionalnim pristupom, u Cloud computing rešenju korisnik koristi informacione tehnologije kao uslugu. U Cloud computing sistemu administratori sistema imaju ulogu partnera čija je uloga da obezbedi da ovakav servis radi po unapred ugovorenim i određenim uslugama. Svrha ovakvog načina pružanja usluge je da se kompanije bave onim što najbolje rade, a da poslove oko informacionih tehnologija prepuste onim kompanijama koje to najbolje rade, čime se smanjuju kapitalna ulaganja i postiže bolji efekat.

U Srbiji pružaoci usluge Cloud computing rešenja su se nametnuli kao lideri u regionu. U Srbiji postoji više pružaoca Cloud computing rešenja među kojima se ističe Telekom Srbije. Zahvaljujući prisutnosti u regionu u Crnoj Gori i BiH ima oko devet miliona pretplatnika i kao provajder signala mobilne telefonije, ali i širokopojasnog Interneta, postavlja se kao idealan partner u ovoj oblasti.

U Srbiji se primenjuje nekoliko modela Cloud computing rešenja koja su bazirana na nekim od navedenih modela :

- Javna Cloud computing rešenja – rešenja sa javno dostupnim servisima koje pružaoci Cloud computing rešenja nude bilo kom korisniku koristeći Internet kao deo usluge.
- Privatna Cloud computing rešenja – Privatni Cloud je rešenje koje je napravljeno isključivo za upotrebu jednog klijenta. Klijent može biti unutar poslovnog sistema ili hostovan od strane pružaoca Cloud computing rešenja. Poslovni sistemi koji imaju privatni Cloud imaju potpunu kontrolu nad strukturom Cloud computing rešenja.
- Zajednička Cloud computing rešenje – Zajednička Cloud computing rešenja su rešenja koja dele nekoliko poslovnih sistema. Infrastruktura ovakvih rešenja podržava posebne zajednice koje imaju zajedničke potrebe, misije i zahteve sigurnosti.
- Spoljašnje Cloud computing rešenje – usluga koja se nudi poslovnim sistemima kao usluga u poslovanju čiji resursi se ne nalaze u sopstvenoj IT organizaciji. Spoljašnja cloud computing rešenja mogu biti javna ili privatna Cloud computing rešenja.
- Hibridno Cloud computing rešenje – predstavlja kombinacija javnog i privatnog Cloud computing rešenja i oslanja se na unutrašnje i spoljašnje IT resurse.

III. DDoS NAPADI

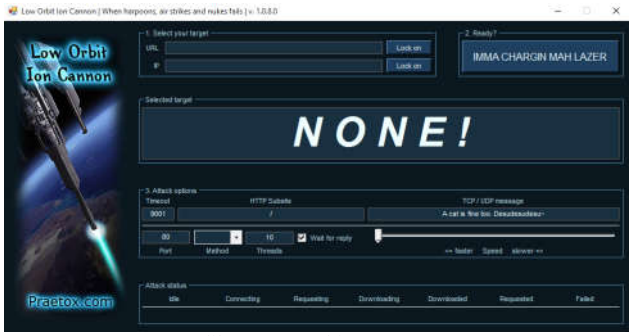
DDoS napadi mogu brzo onesposobiti rad poslovnih sistema i uticati na njihov rad. Motivi i metode DDoS napada su se menjali tokom prethodnih godina, dok je sam cilj napada ostao isti: onemogućiti i otežati korisnicima pristup napadnutim servisima ili resursima. Zajedno sa razvojem sistema zaštite, razvijaju se i sistemi napada. Na samom početku DDoS napada napade je vršio direktno napadač, a svoj identitet je sakrivao tako što je modifikovao početne adrese. Takvi napadi su obuhvatali napade na mreže, sisteme i određene servise prilikom kojih se prema napadnutom resursu slala velika količina neželjenog saobraćaja. Tako usled velike količine informacija i ostvarenog saobraćaja, informacioni sistemi postaju preopterećeni i nisu u stanju da odgovore na regularno poslate upite. Takav sistem rezultuje potpunim prekidom rada ili otežanim pristupom korisnika napadnutim servisima.

Kako je vreme odmicalo DoS napadi su evoluirali u DDoS napade, i to tako što su ulogu direktnih napadača preuzeli računari zaraženi malicioznim softverom, takozvani botovi [4], kojima upravlja napadač preko glavnog računara-servera. Napadač se često krije iza nekoliko proxy servera [5], dok napade bez ometanja izvodi velika grupa korisnika koja čini mrežu napadača. Ovakvi sistemi napada predstavljaju dobar način za povećavanje intenziteta napada jer obuhvataju veliku grupu korisnika, a istovremeno skrivaju direktnog napadača.

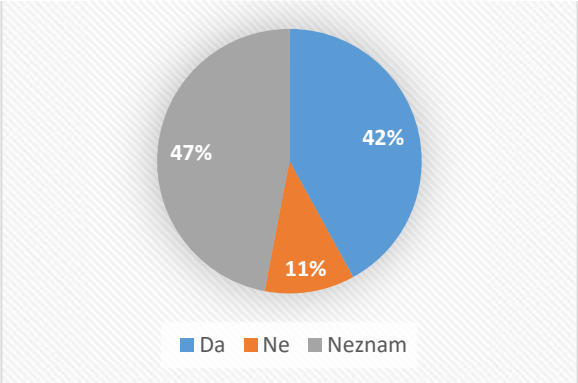
Ovakvi napadi na poslovne sisteme mogu da predstavljaju koordinisane napade više izvršilaca, čiji cilj predstavlja onesposobljavanje samo nekog određenog servisa. Korišćenjem velikog broja izvršilaca, napadač, pored povećanog intenziteta, istovremeno i efikasno krije svoju IP adresu, jer u napadu učestvuje kao koordinator. Ako je broj proxy servera između napadača i žrtve veći, manje su šanse da napadač bude otkriven. Napadi koji danas imaju za cilj da onesposobe informacioni sistem nekog poslovnog sistema uglavnom su DDoS napadi. Najveći razlog napada je lakoća kojom se veliki broj korisnika inficira malicioznim softverom, preko kojeg se vrši napad a i kasnije upravlja napadom.

Upravo veliki broj zaraženih računarskih sistema predstavlja oslonac gotovo svih današnjih DDoS napada. Na ubrzano širenje utiče i brzina razvoja Interneta, nedostatak antivirusnog softvera na korisničkim računarima, ali često i informatička nepismenost korisnika. Individualno posmatrano, svaki zaraženi korisnik ili bot može da pošalje malu količinu saobraćaja, koja ne remeti njegove resurse. Grupno gledano, količina saobraćaja kojom zaraženi korisnici mogu da napadnu ciljanu mrežu direktno je srazmerna njihovom broju. Danas je voma lako doći do alata koji običnom korisniku može da posluži kao alat za jednostavan DoS napad, jedan od alata je i program pod imenom LoIC (eng. Low orbit Ion canon) Sl.1.

Napadači su u stanju da slanjem svega nekoliko komandi upravljaju velikim brojem računara, nekada čak i sa nekoliko hiljada, pa čak i nekoliko stotina hiljada računara zaraženih malicioznim softverom. Maliciozni softver najčešće se širi putem zaraženih računara preko kojih dalje širi maliciozni softver.



Slika 1. Low orbit Ion canon



Dijagram 1. Ispitani poslovni sistemi o trenutnoj zaštićenosti

IV. ZAŠTITA OD DDOS NAPADA

Istraživanje koje smo sproveli nad 220 ispitanih poslovnih sistema u Republici Srbiji otkrilo je da više od trećine ispitanih (38%) poslovnih sistema nisu zaštićeni od DDoS napada, a skoro polovina (49%) se oslanja na alate i hardver koji poseduje za zaštitu (Tabela 1). To nije efikasan način borbe protiv sve većeg broja velikih napada i „pametnih“ DDoS napada koje je teško filtrirati sa standardnim metodama i alatima. Napadi velikih razmera su danas uobičajena pojava, kao što su nedavni napadi ka velikim poslovnim sistemima uključujući Twitter, Guardian, Netflix, Reddit, CNN i mnogih drugih u Evropi i SAD-u.

Problem koji je trenutno uočljiv kod poslovnih sistema je što veliki broj ispitanih pretpostavlja da su već zaštićeni. Gotovo polovina (42%) ispitanih poslovnih sistema misle da je njihov davaoc internet usluga već sve preduzeo u vezi zaštite njihovog informacionog sistema koji ima izlaz na Internet. Veliki deo ispitanih (47%) odgovorio je da nezna da li je njihov poslovni sistem već zaštićen od napada kao ašto je prikazano na Dijagramu 1. Trećina ispitanih (34%) smatra da su njihovi podaci koji se nalaze u Data centrima sigurni od DoS i DDoS napada ali takođe da će im partneri koji pružaju uslugu čuvanja podataka obezbediti nesmetan pristup i zaštitu od ovakvog vida napada. Ovakvi sistemi poslovne sisteme uglavnom štite od masovnog ili standardnog napada, dok 'pametni' napadi, poput onih koji koriste šifrovanje ili oponašaju korisnička ponašanja zahtevaju stručni pristup. Osim toga, istraživanje je pokazalo da trećina (30%) ne poduzima nikakve mere preventivne zaštite, jer misle da verovatno neće biti meta DDoS napada. Začudo, jedan od deset (12%) ispitanih misli da mala šteta naneta ovakvim vidom napada neće izazvati veliki problem za poslovni sistem. Realnost je da bilo koji poslovni sistem može biti cilj DDoS napada jer takvi napadi su veoma laki za pokretanje.

TABELA 1. Zaštita poslovnih sistema

Zaštita poslovnih Sistema		
Pitanje / Odgovori	DA	NE
Da li koristite neki vid zaštite protiv DDoS napada	136	84
Da li posedujete sopstvene alate i opremu	108	112

Ujedno, potencijalni trošak za žrtve može biti veoma veliki, kako u materijalnom tako i u nematerijalnom pogledu.

U napadima izvedenim nedavno, DDoS se pokazao kao vrlo destruktivan. Kada napadači pokrenu DDoS napad, šteta koja nastane može biti poražavajuća za poslovni sistem koji je na udaru jer onemogućuje poslovnim sistemima online prisutnost. Kao rezultat napada, dolazi do zastoja, procesi koji su neophodni za siguran rad ne mogu biti završeni i ugled može biti uništen. Online usluge i IT infrastruktura su previše važni da bi bili ostavljeni nezaštićeni. Zato specijalizovana DDoS rešenja za zaštitu treba smatrati bitnim delom bilo kakve efikasne strategije zaštite u poslovanju danas. Na tržištu danas postoji veliki broj rešenja zaštite od DDoS napada, a neka od takvih rešenja su integrisana i uključuju sve potrebe poslovnog sistema za odbrane od DDoS napada. Ovakva rešenja čuvaju poslovne sisteme tako da njihov informacioni sistem radi glatko i zaštićen je čak i od najsloženijih napada.

V. CLOUD COMPUTING REŠENJA I BEZBEDNOSNI IZAZOVI

IT infrastruktura organizacije je postala veoma teška i kompleksna za zaštitu, pogotovo što se bezbednost zanemaruje u trci za maksimalnim iskorišćavanjem potencijala Interneta. U 2012. godini broj novih virusa bio je veći nego za prethodnih dvadeset godina, da bi taj broj bio nadmašen već u prvoj polovini 2013[4]. Zbog toga se IT organizacije suočavaju sa velikim izazovom, s obzirom da se posao sve više oslanja na Internet. Sudeći po WASC-u , više od 87% Internet aplikacija je ocenjeno kao veoma ranjivo[6]. Kao moguće rešenje ovog problema javljaju se bezbednosni servisi bazirani na Cloudu, koji pružaju inovativan pristup zaštiti podataka organizacije, dodajući globalno raspoređeni sloj odbrane. Ovaj sloj čini razliku u odnosu na centralizovane sisteme i znatno povećava nivo odbrane. Cloud bezbednosna rešenja dozvoljavaju kompanijama da se prilagode rizicima koji se konstantno menjaju, unapred izbegavajući predviđene rizike[7].

Poslovni sistemi svoje podatke danas postavljaju sve češće na Cloud baziranim sistemima. Ovakvo okruženje predstavlja dobar polazni osnov za odbranu od DDoS napada. Odbrana u ovakvom sistemu podrazumeva razvijanje preklapajućih bezbednosnih slojeva koji koriste različite taktike zaštite protiv napada.

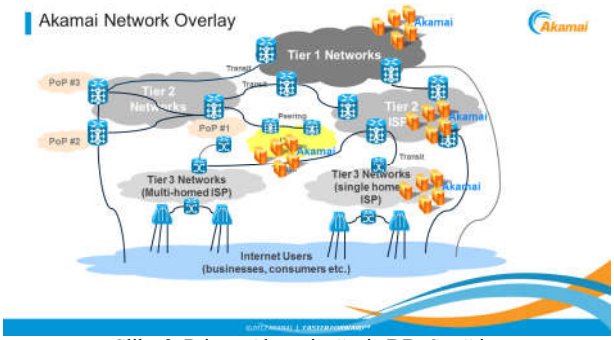
U tabeli 2. su prikazana najaktuelnija rešenja za borbu protiv DDoS napada. Dva rešenja koja se izdvajaju po zastupljenosti u Republici Srbiji su rešenja Akamai, prvobitno razvijenom na Masačusetsovom Tehnološkom Institutu (MIT) i CloudFlare rešenje osnovano od strane Matthew Prince, Michelle Zatlyn i Lee Holloway.

Akamai rešenje za odbranu od DDoS napada u Cloud computing rešenju je alat iza kojeg stoji stručan tim koji pruža proaktivno praćenje, pomoć oko konfigurisanja i podršku stručnog tima za bezbednost. Akamai je servis koji omogućuje pristup Akamai sigurnosnim stručnjacima i obezbeđuje siguran monitoring. Servis proaktivno upozorava na pretnju koja može da bude izazvana DDoS napadim. Upravljanje incidentnom situacijom korisnik usluge može samostalno da rukovodi ili da ga prepusti stručnom timu Akamai ili u saradnji sa njima preuzme potrebne korake. Proaktivno nadgledanje bezbednosnih aspekata predstavlja okosnicu ovog alata Sl. 2.

Drugo rešenje koje se nameće, kao lider u borbi protiv DDoS napada, je istoimeno rešenje kompanije CloudFlare. Ovo rešenje se izdvaja od ostalih po tome što sistem velikim delom radi automatski i prepoznaje DDoS napad izazvan na samom početku (Sl. 3).

TABELA 2. Uporedni prikaz rešenja za odbranu Cloud baziranih rešenja od DDoS napada

Naziv rešenja	Cloud	Tradicionalni
CloudFlare	X	X
BitNinja	X	X
Imperva Incapsula	X	
JavaPipe	X	
Akamai	X	X
Dynu Dynamic DNS	X	X
ClouDNS	X	



Slika 3. Primer Akamai rešenja DDoS zaštite

Napredna zaštita od DDoS napada CloudFlare radi kao servis na kraju mreža, prepoznaje sofisticiranost i obim ovakvih pretnji i može da se koristi kako za sprečavanje, tako i za ublažavanje DDoS napada svih oblika i veličina uključujući i one napade koji su usmereni na UDP i ICMP protokole.

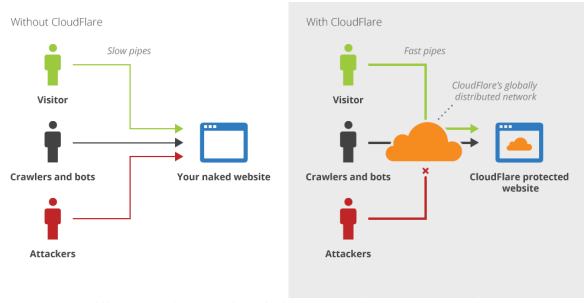
CloudFlare je jedna od najvećih mreža za zaštitu od DDoS napada u svetu. Zaštita je bazirana na flat-rate zaštiti od DDoS zasnovanu na tehnologiji „anicast“ i može uspešno da ublaži napade veće od 400Gbps.

Skoro deceniju, softverske kuće koje se bave proizvodnjom sigurnosnih mehanizama čine Internet boljim, bržim i sigurnijim mestom za poslovanje. Veliki broj kompanija se oslanja na isključivo softverska rešenja kako bi osigurale i ubrzale svoje online transakcije koristeći platformu koja obezbeđuje sigurnost na ivicama Cloud computing rešenja. Edge Platforma, kako se drugačije zovu rešenja koja se oslanjaju na mehanizme koji se nalaze na ivicama Cloud computing rešenja je dokazana platforma za pružanje inteligentne i skalabilne odbrane koja štiti od širokog spektra napada, bio to napad na DNS infrastrukturu organizacije, mrežni sloj ili internet aplikaciju. Obiman i fleksibilan skup sposobnosti može se prilagoditi različitim vrstama pretnji i napada na zahtev. Softverska rešenja omogućavaju korisnicima da u potpunosti uživaju u mogućnostima Cloud computing rešenja, održavajući kontinuitet poslovanja.

Odbrana od DDoS napada sa ovakvim sistemima se svodi na odbranu iz pet delova :

1. Filter IP različitosti,
2. Filter broja skokova,
3. Filter dvostrukog potpisa
4. Filter senzora,
5. Filter „puzzle resolver“.

Svi filteri detektuju HTTP DDOS napade jedino filter „dvostrukog potpisa“ detektuje XML-bazirane napade. Jedan od najproblematičnijih DDoS napada je REST-bazirani napad. Trenutno su sva prisutna rešenja bez nekog konkretnog rešenja za njihovo zaustavljanje. Jedan od razloga je taj što su REST-bazirani napadi blisko povezani sa korisničkim interfejsom, koji može varirati od korisničkih pa do sistemskih aplikacija. Te aplikacije su po svojoj prirodi drugačije, na osnovu toga šta se od njih traži i čemu su namenjene, tako da ne postoji jedinstveno pravilo za implementaciju bezbednosnih mera na tom nivou.



Slika 2. Primer CloudFlare rešenja DDoS zaštite

Rešenje se sastoji iz sledećih modula:

- Senzor
- Filter broja skoka
- Filter IP različitosti
- Dvostruki potpis
- „Puzzle solver“

Senzor: Prati dolazeće poruke sa zahtevima. Ako senzor odredi da postoji povećanje zahteva od određenog korisnika, on ga označava kao sumnjiv.

Filter broja skokova: Služi za brojanje vrednosti broja skokova (koliko čvorova, da li poruka putuje od izvora do odredišta) i upoređuje sa predefinisanim brojem skokova. Ako postoji razlika u broju, to znači da postoji mogućnost da je zaglavlje poruke ili poruka promenjena na kompjuteru napadača i zato se označava kao sumnjiva.

Filter IP različitosti: Obeležava poruke sumnjivim ako se šalje veliki broj poruka sa iste IP adrese.

Dvostruki potpis: Udvostručuje XML potpise. Jedan potpis se nalazi u zaglavlju a drugi na kraju poruke. U slučaju napada, neophodno je proveriti oba XML potpisa.

„Puzzle Solver“: Ovaj filter funkcioniše po sistemu rešavanja slagalice, gde je rezultat uključen u zaglavlje SOAP (Simple Object Access Protocol) protokola. U slučaju napada (HTTP DDOS), cloud defender će pošiljaocu poruke poslati da reši slagalicu na zadatu IP adresu. Ako cloud defender primi rešenu slagalicu onda se poruka i IP adresa obeležava kao sigurna, u suprotnom se obeležava kao HTTP DDOS napad[9].

Nedostatak ovog sistema jeste što zahteva iscrpno praćenje svih poruka što bi znatno usporilo tok saobraćaja u mreži. Konačno, sistem nema mehanizam upravljanja čvorovima u slučaju detekcije napada. Od nedavno je pitanje interne pretnje sve aktuelnije. Napadači su svesni da mogu da planiraju napad na Cloud baziranom sistemu iznajmljivanjem velikih količina resursa iznajmljenog Cloud computing rešenja i potom da sam napad sprovedu u drugi deo Cloud baziranog rešenja ili na neku tačno određenu virtuelnu mašinu koja se nalazi u istom Cloud computing rešenju. Rešenje koje se nameće u ovakvim slučajevima jeste pravilno i stručno konfigurisanje firewall uređaja unutar same mreže pružaoca usluge Cloud computing rešenja i to predstavlja jedini i ključni deo odbrane od ovakvog vida napada.

Akamai i CloudFlare rešenja imaju zajedničku odliku a to je sistem za detekciju upada. Napadači, koji se predstavljaju kao obični korisnici, mogu pristupiti Cloud computing infrastrukturi, pri čemu infrastruktura postaje nedostupna korisnicima. U praksi se pokazalo da napadač može jednostavno doći do podataka sa računara koje je napao kod IaaS servisa[8]. Ovakvi podaci mogu pomoći u napadu na Cloud bazirane sisteme. Ti napadi se obično sastoje i iz DoS i DDoS napada kojima se ugrožava integritet i dostupnost podataka. Ovakvi napadi se izbegavaju implementacijom nekog od predloženih sistema za detekciju upada. Ovakav sistem automatski analizira mrežni saobraćaj kroz log fajlove i ponašanja korisnika. Akamai i CloudFlare rešenja definišu se kao sistemi koji sakupljaju i analiziraju podatke bezbednosnih razlika kako bi proverili da li postoji prekršaj mrežnih pravila.

Detekcija upada se može klasifikovati u dve kategorije:

- Detekcija zloupotreba i
- Detekcija anomalija

Detekcijom zloupotreba stavlja se naglasak na karakteristike podataka korisnika i upoređuju se sa rezultatima iz baze podataka. Komponenta detekcije anomalija čuva korisničke navike u bazi podataka, a zatim se vrši upoređivanje sa trenutnim navikama. Posle izvršene analize, ako postoji velika razlika u upoređivanju, sistem detektuje napad i obaveštava korisnika o istom.

Postoje više vrsta sistema za detekciju DDoS napada, ali izdvojićemo tri :

- Sistem koji je zasnovan na jednom računaru, usmereno se prati samo jedan računar HIDS (eng. - Hostbased Intrusion detection system)
- Mrežni sistem, analiza protoka se vrši na svim računarima u mreži NIDS (eng. - network-based intrusion Detection system - NIDS)
- Hibridni sistem, zasnovan na kombinaciji prethodna dva.

Navedena dva sistema predstavljaju vrstu sistema za detekciju upada koji radi sa predefinisanim ali i naučenim pravilima. Na osnovu definisanih pravila sistem se samostalno i automatski konfiguriše (povećava protok, procesorsku snagu), ali takođe se i samostalno oporavlja. Ovakvim sistemom se smanjuje uticaj čoveka na kompletan sistem. Pravila se definišu metodama upravljanja ali i veštačkom inteligencijom. Bez samostalnog sistema nemoguće je upravljati distribuiranim sistemima najnovije generacije Cloud computing rešenja.

Sistem koji je namenjen ovakvom vidu odbrane od DDoS napada naziva se i Security audit. To je samostalni, inteligentni, autonomni sistem namenjen za detekciju incidenata i napada. Oba sistema navedena u radu spadaju u ove sisteme. Daje se pretpostavka da je korisnik svestan toka instanci u razvijenom Cloud computing sistemu. CloudFlare prikuplja podatke direktno sa izvora, analizira i prikuplja informacije a zatim ih prosleđuje. Centralni deo sistema je zasnovan na analizi podataka koji se vrši na nivou ugovora servisa sigurnosti (SSLA). CloudFlare prepoznaje tri osnovna problema zasnovanih na Cloud computing platformi:

- Nedozvoljene radnje iz cloud resursa,
- Nedovoljnog praćenja Cloud computing strukture,
- Loša izdvojenost deljenih resursa.

CloudFlare i Akamai rešenja koriste veliki broj oslušivača kojima prepoznaju promene u sistemu. Oslušivači primaju uputstva i bezbednosne polise od samog sistema. Iako su CloudFlare i Akamai autonomni alati, bezbednosna politika je ipak zasnovana na pravilima koja su unapred definisana, time se prepoznavanje napada ograničava na napade koji su se već dogodili a sistem ih je prepoznao i postavio u svoju bazu kao

jedan od načina izvršenja napada. Akamai sadrži veliki broj agenata, funkcija i podalata čime se sa druge strane postiže veliki saobraćaj u sopstvenoj mreži, kako zbog međusobne komunikacije, tako i zbog ukupnog saobraćaja, a time se i troškovi Cloud computing servisa povećavaju. Potpuni autonomni sistem u svojoj arhitekturi mora posedovati autonomnog menadžera, koji je sposoban da pravi i izvršava planove implementacije. Plan bi trebalo da bude zasnovan na primljenim i poslatim informacijama.

Ova dva sistema opisana u radu koriste i informacije koje dobijaju od čvorišta u realnom vremenu. Polise su automatizovane i decentralizovane sa glavnog na sva sporedna čvorišta. Ovakvi sistemi imaju pod sobom još nekoliko komponenti :

- Repozitorijum virtuelnih mašina – interfejs kojim se upravlja virtuelnim mašinama i istovremeno kreira URL za svaku pokrenutu virtuelnu mašinu.
- Cloud kontroler – komponenta koja određuje koja virtuelna mašina odgovara svakom pojedinačnom klijentu,
- Cloud agent – inteligentni softver koji odgovara na upite cloud kontrolera. Pitanja se odnose na dostupne konfiguracije virtuelnih mašina za određeni period iznajmljivanja tih mašina,

Cloud agent se sastoji iz nekoliko delova, kao što je :

- Menadžer sposobnosti,
- Menadžer zahteva,
- Menadžer polisa,
- Skladištenja podataka.

Bitni elementi zbog koga se CloudFlare i Akamai sistem razlikuju od drugih sličnih sistema je što sadrže decentralizovano upavljanje polisama, dok većina drugih sistemi imaju master-slave arhitekturu koja predstavlja usko grlo sistema. Kod ovog pristupa, ako se nešto dogodi sa master elementom, sistem može otkazati delimično ili čak u potpunosti. Ovakav problem se rešava upravo decentralizovanim pristupom. Polise se prenose sa glavnog na lokalna čvorišta. Zbog brzih promena u Cloud computing tehnologiji, neophodno je da decentralizacija bude potpuno samostalna. Decentralizacijom upravljanja polisama se postiže povećana pouzdanost i bezbednost, jer ako je jedno čvorište ugroženo, ostala čvorišta mogu nesmetano obavljati svoje zadatke.

VI. RAZVIJANJE TRŽIŠTA BEZBEDNOSTI

1 Tbps DDoS napadi na Cloud computing rešenja će postati osnova za "masovne napade". Pre četiri godine najveći napadi su bili od 65 Gbps. Naredne godine napadi su ponovljeni ali sada sa 300Gbps a jedan od razloga je i brzina Interneta koja se povećala, samim tim i DDoS napadi. U 2016. godini su bili sporadični napadi od 1Tbps koje su prijavili različiti pružaoci usluga. Pretpostavlja se da će u 2017. godina osnovica za masovne napade biti 1Tbps.

Iako HTTP/2 protokol ima veliki uticaj na veb performanse, to zavisi i od TCP protokola, što može dovesti do problema sa performansama direktnih Internet veza. Google je eksperimentisao sa protokolom koji se zove QUIC, koja koristi UDP umesto TCP. U 2017. godini očekuje se da se razvoj ovakvog protokola nastavi i da postane smer razvoja.

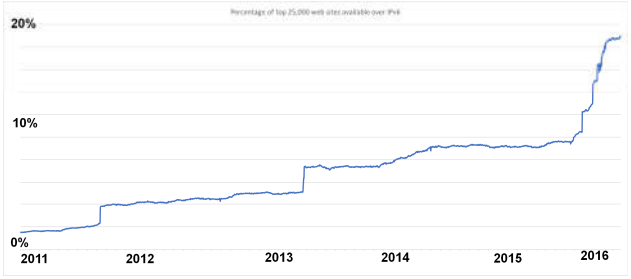
Tržišna predviđanja pretpostavljaju da će IPv6 postati upotrebljiv jedino za mobilne mreže, dok će IPv4 koristiti isključivo fiksne mreže.

Podaci dobijeni od kompanije Techcrunch govore da je IPv6 protokol 27% brži, Facebook 10% do 15% brži, LinkedIn između 10%- 40% procenata brži na mobilnim uređajima nego na računarima sa fiksnom vezom i Ipv4. Bez obzira koliko procenata je neki portal brži, jasno je da IPv6 pruža veće brzine. Dijagram 2. pokazuje procenat prvih 25.000 sajtova (prema Alexa) koji su dostupni preko IPv6. DDoS napadi su obično bili volumetrijski napadi na slojevima 3 i 4 (kao što je SIN prelivanje). Verujemo da će Laier 7 napadi (naročito preko HTTP i DNS protokola) nastaviti da rastu u 2017. Istovremeno se očekuje da se pojave i Laier 7 napadi na protokol TLS (eng. Transport Layer Security). Takvi napadi su se već dešavali u prošlosti, to su napadi koji su dizajnirani da troše CPU servera zadajući im da reše kompleksne kriptografske operacije.

VII. ZAKLJUČAK

Poslednjih godina, bezbednost i sigurnost na Internetu je glavna i najvažnija tema. Napadi postaju sve kompleksniji i sofisticiraniji, intenzivniji i učestaliji što zahteva praćenje trendova u odbrani od ovakvog vida napada. To pokazuju i analize i statistika DDoS napada.

Činjenica je, dakle, da je visoko-tehnološki kriminal i tzv. sajber-kriminal i kod nas i u svetu u porastu. Posredni gubici nastali usled izgubljenog posla, izgubljenih klijenata ali i trošak oporavka sistema kao i gubitak reputacije pouzdanog partnera su ozbiljni razlozi koji teraju poslovne sisteme da pored ugovora sa svojim pružaocem usluge Cloud computing rešenja o zaštiti od DDoS napada započnu implementaciju alata za rano prepoznavanje ovakvog vida napada. Cloud computing rešenje kao rešenje naročito je bitno za posao, kao takvo mora se i adekvatno zaštititi i smestiti na što sigurnije mesto.



Dijagram 2. Procenat 25,000 sajtova baziranih na Cloud computing rešenju

LITERATURA

[1] Alargić P, Kaurin T, : "Sigurnosni problemi u Cloud computing rešenju", INFOTEH-JAHORINA Vol. 13, March 2014, Published

[2] http://www.gartner.com/it-glossary/cloud-computing/, accessed 25.12.2016

[3] NIST Tech Beat : “Final Version of NIST Cloud Computing Definition”, October 25, 2011, Published

[4] https://botizam.wordpress.com/2011/02/19/izvorna-smisao-rijeci-bot/, accessed 12.01.2017

[5] Peng T, Leckie C, Ramamohanarao K, : “Survey of network-based defense mechanisms countering the DoS and DDoS problems”, ACM Computing Surveys (CSUR) Surveys,Volume 39 Issue 1, 2007

[6] WASC Announcement : “Static Analysis Technologies Evaluation Criteria”, 2013, Published

[7] Alargić P, Kaurin T, : “Sigurnosni problemi u Cloud computing rešenju”, INFOTEH-JAHORINA Vol. 13, March 2014, Published

[8] P. Alargić: “Unapređenje poslovanja primenom Cloud computing tehnologije”, IV međunarodni naučni skup Multikulturalnost i savremeno društvo u Novom Sadu, 2013. Published

[9] Popović O, : „Energetski efikasno rešenje platforme za mobilno učenje u cloud computing okruženju“, Doktorski rad, Univerzitet Singidunum, Beograd, 2016. Published

ABSTRACT

Security incidents are increasingly present on the Internet, if we take into account not only those which compromise end-users, but also those who attack large computer systems, such as companies with multinational operations, the state authorities as well as Internet service providers. Malicious attacks that are aimed at end users almost always come as a malicious program that degrade user performance computer and has the ability to collect sensitive data. The attackers almost always via malicious software take control of the computers that are infected, in order to carry out a coordinated attack. The infrastructure provided by Internet service providers, government agencies or large companies use a lot of users. The end result of these attacks is almost always a large scale. In this paper, with reference to the DDoS attacks and Cloud computing solution as one of the solutions, analyze the reliability of cloud computing solutions in the incidents.

ANALYSIS OF THE RELIABILITY OF CLOUD COMPUTING SOLUTIONS TO DDOS ATTACKS

Predrag Alargić, Tanja Kaurin