Ekipa iz Arbor Networksa potrudila se da nam u kratko vrijeme pruži što bolji uvid u proizvode svoje kompanije

DDoS pod kontrolom

Američka tvrtka Arbor Networks u Zagrebu je demonstrirala svoja moćna rješenja za borbu protiv DDoS napada

Rajko Plečko

U zagrebačkom hotelu Esplanade, u organizaciji Veracompa, održano je druženje sadašnjih i potencijalnih korisnika sa specijalistima tvrtke Arbor Networks, s ciljem predstavljanja novih proizvoda i servisa koje na svjetskom tržištu trenutačno nude, a koji su zanimljivi svakoj organizaciji koja drži do vlastite sigurnosti u internetskom okruženju.

Kompanija Arbor Networks osnovana je 2000. godine u Massachusettsu kao *spinoff* istraživačkog projekta na univerzitetu Michigan, koje su sponzorirali DARPA, Cisco i Intel. Profesori Farnam Jahanian i Rob Malan, uz podršku nekolicine studenata, formirali su tvrtku čiji su glavni proizvod sustavi za mrežnu sigurnost i softver za nadzor mreže koji je, kako tvrde, u pogonu pri više od 90% svih pružatelja internetskih usluga. Tu su se usko specijalizirali na zaštitu od DoS (Denial of Service) napada, botnetova i računalnih crva, te drugih napada koji za cilj imaju onesposobljavanje *routera* mrežnog prometa. Arbor je danas dio korporacije Netscout Systems, koju uz njih čine Tektronix Communications i Fluke, preuzeti od korporacije Danaher.

MAGNITUDE NAPADA I DO 1,7 Tbit

Druženje je otvorio Aleksandar Stančin, direktor prodaje sigurnosnih sustava u Veracompu, koji je nakon kratkog predstavljanja svoje tvrtke kao značajnog VAD-a (Value Added Distributer), na području koje čine sve zemlje nastale raspadom Jugoslavije, i onog dijela svijeta koji smo nekada kolokvijalno zvali Istočnom Europom, riječ predao Marku Đorđeviću (Regional Sales Manager) i Marcu Gianoli (Senior Consulting Engineer and Service Architect) iz Arbor Networksa.

Budući da je jedna od najvažnijih problematika koju Arborovi istraživački napori adresiraju, zaštita od DDoS napada, za početak smo čuli podatak da je magnituda najžešćeg napada u posljednjih godinu dana iznosila otprilike 1,7 Tbit/s, i to protiv neimenovanog pružatelja internetskih usluga u SAD-u, a dogodila se samo tjedan dana nakon nešto slabijeg napada od 1,3 Tbit/s na GitHub, koji ga nije bio u stanju izdržati.

Teško je zamisliti takvu količinu prometa usmjerenu prema jednoj točki, **a još teže metodu obrane protiv takvog napada i scenarij kako ga** "preživjeti". Mogli bismo se zapitati i čemu tolika panika oko svega, kad takvi napadi najčešće traju vrlo kratko, a nakon toga se sve vraća u normalu.

Spomenut ćemo primjer iz prezentacije koji ovu paranoju dobro ilustrira. Zamislimo da se radi o napadu na, primjerice, *online* kladionicu u trenutku prije početka važnog meča ili utakmice, kad se uplaćuju posljednje oklade. Ako napadač onemogući raspoloživost web-stanice koja prima uplate, igrači će se vrlo vjerojatno okrenuti nekoj drugoj kladionici kojoj je pristup moguć. Dakle, za samo nekoliko desetaka minuta učinjena je ogromna materijalna šteta jednom subjektu i korist nekom drugom pa napad može prestati. Strah od takvih napada trebao bi biti još i veći, ako znamo da na webu postoje servisi gdje takav napad možete "kupiti" već za nekoliko dolara. Sve što trebate znati jest koliko intenzivan napad želite, u koje vrijeme, koliko dugo želite da traje i, naravno, tko će biti cilj napada.

Raspored čvorova Arbor Networks Clouda, propusta 9,4 Tbit/s, koji je u stanju nositi se i s najvećim dosad zabilježenim napadima

RJEŠENJE

Arbor Networks nudi rješenje za ovakve crne scenarije u raznim oblicima. Od "malih" uređaja, koje možete smjestiti u svoju mrežu i sami se na svojem terenu boriti protiv napadača, ako mrežne servise *hostate* sami, do svojeg distribuiranog *cloud* sustava za analizu prijetnji pod imenom ATLAS (Active Threat Level Analysis System), koji ima izvrsne mehanizme i dovoljnu propusnost da se izbori i s najgorim napadima. Radi se o sustavu koji sakuplja podatke od gotovo svih vodećih ISP-ova. Svi ti pružatelji usluga šalju informacije o prometu koji prolazi kroz njihove uređaje, uključujući i stotine manjih ili većih DDoS napada, koje zamjećuju na svojoj mreži. Podaci se sakupljaju i iz njih se generiraju trendovi, koji onda daju detaljnu sliku na globalnoj razini. Iz svega prikupljenog mogu se vidjeti magnituda i učestalosti napada prema regijama, pojedinim državama ili IP adresama. Sve to pruža mogućnost ISP-ovima da se upoznaju s prijetnjama i za njih bolje pripreme, kako bi nanijele što manju štetu ako se realiziraju.

Ako ste uslugu zaštite kupili preko svojeg ISP-a, a postali ste metom jednog takvog napada, kompletan se promet prema vama automatski preusmjerava prema Arborovom *cloudu*, koji će ga u realnom vremenu očistiti od svega što ne predstavlja korisne podatke, i vratiti vašoj mreži. Kako se to radi vrlo visoko u mrežnoj hijerarhiji, vjerojatno je da, osim činjenice da se incident dogodio, druge efekte nećete ni primijetiti.

Sustavi Arbor Clouda trenutačno su razmješteni na 14 lokacija u svijetu i mogu podnijeti 9,4 Tbit/s prometa. To je brojka koja još neko vrijeme sigurno neće biti dostignuta, pa pruža vrlo visoku razinu sigurnosti. M