Žarko Kecić,
izvršni direktor za IKT, RNIDS

Sigurnost DNS servisa

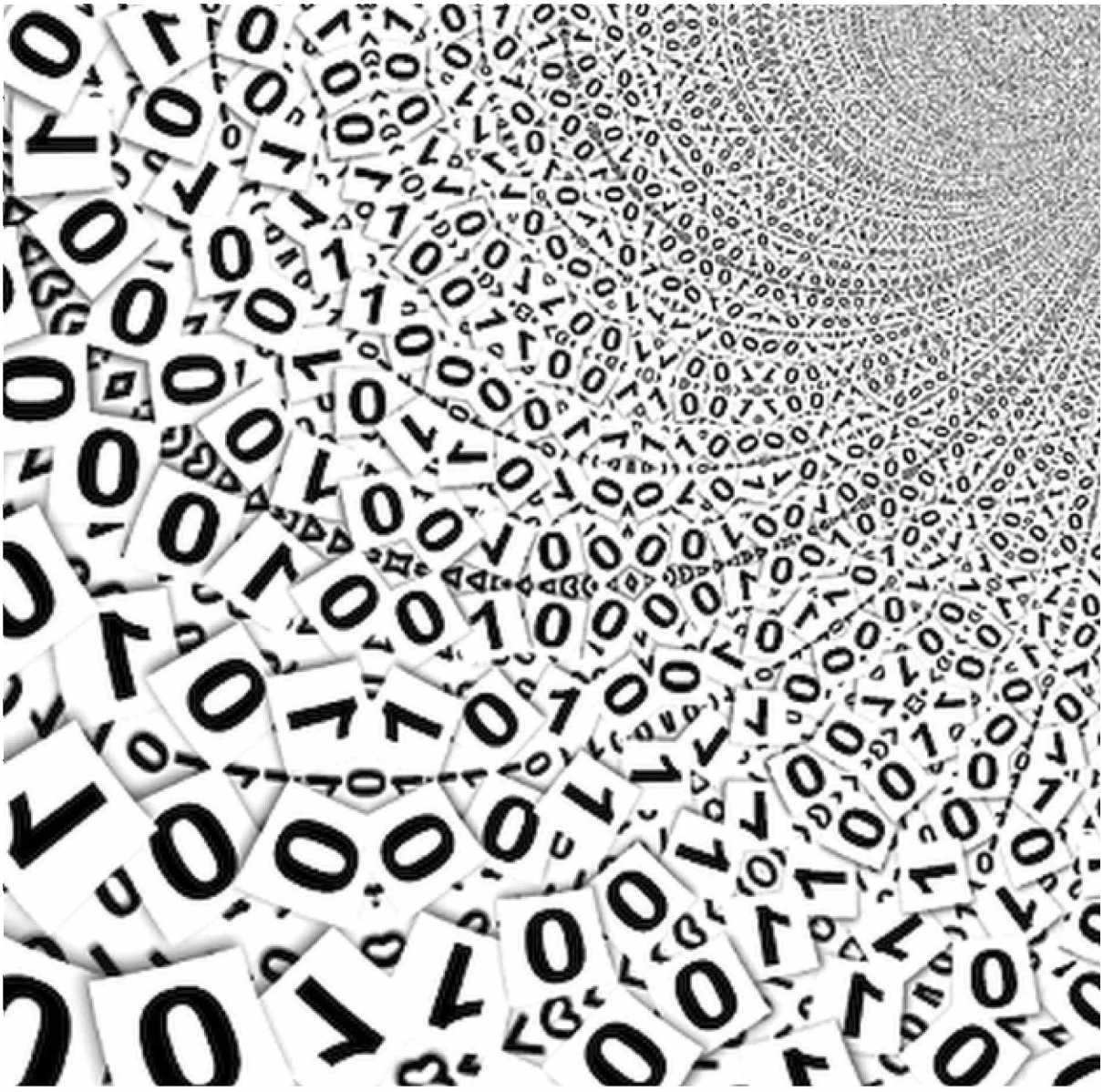
DNS servis je jedini centralizovan i hijerarhijski organizovan servis na internetu. Uz to, DNS servis se od svog nastanka veoma malo menjao. Stoga je razumljivo da DNS serveri, zbog svog značaja, predstavljaju stalnu metu zlonamernih korisnika interneta. Ciljevi napadača mogu biti različiti, od političkih i verskih do materijalnih, ili jednostavno destruktivnih.

Sobzirom da većinu korisnika ne zanimaju tehnički detalji rada DNS-a, ovom servisu nije posvećena dovoljna medijska pažnja, nije sprovedena edukacija korisnika o njegovom značaju, a kako se u poslednje vreme pokazalo, nije ni ukazano na njegove slabosti koje otvaraju nove mogućnosti za zlonamerno delovanje na Internetu. Čak i mnogi računarski obrazovani korisnici, pa i sistem administratori, smatraju DNS jednostavnim i dosadnim i ne posvećuju mu pažnju koju, zbog svog značaja za funkcionisanje Interneta, s pravom zaslužuje.

I cilj i sredstvo napada

Loše konfigurisani i neobezbeđeni DNS-ovi mogu biti iskorišćeni na različite načine, bilo kao direktni ciljevi napada ili kao sredstvo za napad na druge računarske sisteme bilo gde u svetu.

Poslednjih meseci u udarnim vestima o napadima na sisteme velikih banaka, medijskih kuća i vodećih svetskih kompanija može se čuti i pročitati da su napadači koristili loše



konfigurisane DNS servere ili su na neki način, u DNS sistemima, izmenili IP adrese internet servisa koji su bili meta napada.

Krajem marta, svetom je prostrujala vest da je na anti-spam provajdera Spamhaus izvršen najveći DDoS (Distributed Denial of Service) napad u istoriji Interneta. Za napad je optužen holandski hosting provajder Cyberbunker, čiji su serveri za slanje elektronske pošte prethodno stavljeni na crnu listu od strane Spamhausa. Kako je moguće da jedan hosting provajder generiše saobraćaj od preko 300 Gb u sekundi?

Prema izveštaju Open Resolver Project, u svetu ima više od 20 miliona loše konfigurisanih i neobezbeđenih DNS servera koji mogu biti iskorišćeni kao "pojačavači" napada, koji generišu mnogostruko veću količinu podataka od inicijalne. Naime, standardni DNS upit je veličine oko 30 bajtova, dok odgovor koji šalje DNS server može biti od 100 do 200 puta veći. Obično se DNS upit šalje putem UDP protokola koji ne zahteva uspostavljanje dvosmerne komunikacije, što omogućava napadačima

da se lažno predstave (spoofing) i predstave da upit dolazi sa IP adrese žrtve napada a ne sa IP adrese sa koje je u stvari poslat. DNS server u odgovoru šalje znatno veću količinu podataka, ali na IP adresu žrtve. Ako uzmemo u obzir da je jedan DNS server u stanju da obradi i pošalje odgovore na stotine hiljada DNS upita u svakoj sekundi, onda možete zamisliti koliki saobraćaj može proizvesti nekoliko stotina, pa i hiljada, loše konfigurisanih DNS servera. Cloudflare je objavio da je u prošlogodišnjem napadu na njihovu internet infrastrukturu, koji je po obimu bio znatno manjeg intenziteta od napada na Spamhaus, učestvovalo više od 65.000 DNS servera.

Drugačiji scenariji

Pre nešto više od mesec dana izveden je još jedan napad koji se odnosi na DNS servere, ali drugačije koncipiran. Napadači, koji se predstavljaju kao Syrian Electronic Army (SEA), uspeli su da, koristeći prava pristupa partnerske firme za registraciju internet domena, promene podatke u DNS sistemu poznatog australijskog provajdera Melbourne IT i na taj način preusmere internet korisnike velikog broja poznatih kompanija, među kojima su New York Times, Washington Post, Financial Times, Twitter, i neke servise BBC-a, AP-a i Reutersa, ka serverima koji su pod kontrolom napadača. Pretpostavlja se da je ovaj napad imao za cilj samo političku "vidljivost" na Internetu, ali ovaj i slični napadi mogu imati mnogo veće i ozbiljnije posledice.

Preusmeravanje Internet saobraćaja, recimo New York Timesa, znači i mogućnost preusmeravanja elektronske pošte na servere koji su kontrolisani od strane napadača, a samim tim i otvoren pristup elektronskoj komunikaciji putem e-maila. U slučaju Melbourne IT takva promena je bila brzo primećena, ali je veoma verovatno da bi takav scenario kod manje opreznih DNS operatera bio otkriven tek danima, a možda i mesecima, kasnije.

Poznato je da su česti slučajevi preusmeravanje korisnika online servisa na Internet lokacije koje kontrolišu napadači i koje se po svom izgledu i sadržaju ne razlikuju od originalnih servisa kojima je korisnik želeo da pristupi. Mnogo je načina za realizaciju ovakvih napada, ali je izmena DNS zapisa online servisa banaka, Internet prodavnica i drugih servisa gde se od korisnika traži da unesu osetljive podatke o svom identitetu ili brojeve kreditnih kartica i bankovnih računa, čest i veoma efektivan način da se u kratkom vremenskom roku "prevari" veliki broj korisnika.

Tipovi napada

Najčešći tipovi napada na DNS servis su

· DoS i DDoS napadi

· Upotreba DNS servera za amplificirani DDoS napad na druge internet servise

· Presretanje i izmena DNS paketa (man in the middle)

· "Trovanje keša" (cache poisoning)

· Izmena DNS zapisa i zonskog fajla