



---

FAKULTET ZA POSLOVNU INFORMATIKU

---

Djordje Antić

# **BEZBEDNOST ADRESIRANJA RAČUNARA NA INTERNETU**

**- Diplomski rad -**



---

FAKULTET ZA POSLOVNU INFORMATIKU

---

# **BEZBEDNOST ADRESIRANJA RAČUNARA NA INTERNETU**

**- Diplomski rad -**

Mentor:  
Prof. dr Mladen Veinović

Student:  
Djordje Antić

Br. indeksa:  
8n/2004



---

## FAKULTET ZA POSLOVNU INFORMATIKU

---

**UNIVERZITET SINGIDUNUM**  
**FAKULTET ZA POSLOVNU INFORMATIKU**  
**Beograd, Danijelova 32**

Broj: \_\_\_\_\_/2008

**Kandidat:** Djordje Antić

**Broj indeksa:** 8n/2004

**Smer:** Projektovanje i programiranje

**Tema:** BEZBEDNOST ADRESIRANJA RAČUNARA NA INTERNETU

**Zadatak:** Opisati funkcionisanje sistema imenovanja domena (DNS), načina da se on obezbedi, njegovih trenutnih slabosti i nedostataka kao i zloupotreba od strane pojedinaca i kriminalnih grupa. Posebnu pažnju posvetiti trenutno najvećoj pretnji za bezbednost na Internetu – *bot* mrežama i *fast-flux* tehnici. Takođe, uzeti u obzir sve aspekte koje obezbeđivanje DNS-a podrazumeva, kako za krajnje korisnike, tako i za tela koje će se baviti ovim zadatkom.

**MENTOR**

---

Prof. dr Mladen Veinović

**Datum odobrenja teme:**  
09.05.2008.  
Beograd

**DEKAN**

---

Prof. dr Milan Milosavljević

**Sažetak:** Sistem imenovanja domena (DNS) je temelj na koji se oslanja većina mrežnih aplikacija, kao i sama bezbednost mreže. Međutim, sam sistem nije projektovan da bude bezbedan, što danas predstavlja potencijalno veliku pretnju za bezbednost na mreži, uz pojedince i kriminalne grupe koje iskorišćavaju njegove nedostatke. Predloženo rešenje u vidu bezbednosnih proširenja DNS-a (DNSSec) rešava neke bezbednosne probleme, ali ne i određene sofisticirane tehnike zloupotrebe (*fast-flux bot* mreže, DDoS) koje danas čine najveći i najopasniji deo sajber-kriminala na Internetu. Na kraju, postoji i pitanje, političko isto koliko i tehničko, kontrole i samim tim moći koju obezbeđjivanje DNS-a donosi telu koja bi dobilo taj zadatak – pitanje koje u današnjem svetu ima veoma kontroverznu konotaciju.

**Abstract:** The domain name system (DNS) is the foundation on which most network applications, as well as network security, relies. However, the system itself was not designed to be secure, which represents potentially significant threat to online security today, with individuals and criminal groups exploiting the system's shortcomings. Suggested solution in the form of DNS Security Extensions (DNSSec) resolves some security issues, but not certain sophisticated abuse techniques (*fast-flux bot* networks, DDoS) that make the largest and most dangerous part of cyber-crime on the Internet today. Finally, there is also the issue, political as much as technical, of control and power that securing of DNS provides to the body that would perform the task – issue that has a very controversial conotation in the world as it is today.

*Bezbednost nije samo cilj,  
ona je apsolutno neophodna.*

Daniel J. Bernstein

## Sadržaj

---

|                                                   |        |
|---------------------------------------------------|--------|
| Uvod .....                                        | - 1 -  |
| 1. Pregled DNS-a.....                             | - 2 -  |
| 1.1 Struktura DNS-a.....                          | - 2 -  |
| 1.2 Struktura DNS podataka.....                   | - 5 -  |
| 2. Mehanizmi za obezbedjenje DNS-a .....          | - 7 -  |
| 2.1 DNSsec .....                                  | - 7 -  |
| 2.2.1 Funkcionisanje DNSsec-a.....                | - 7 -  |
| 2.2.2 Slabosti DNSsec-a.....                      | - 8 -  |
| 3. Bezbednosni problemi DNS-a.....                | - 10 - |
| 3.1 DNS lažiranje .....                           | - 11 - |
| 3.2 Prevara od strane servera kome se veruje..... | - 13 - |
| 3.3 Napad radi blokiranja usluga .....            | - 15 - |
| 3.4 Bot mreže .....                               | - 16 - |
| 3.5 Fast flux .....                               | - 20 - |
| 3.5.1 Storm bot mreža .....                       | - 25 - |
| 3.5.2 DDoS Funkcionalnost .....                   | - 27 - |
| 3.5.3 Šifrovanje i prodaja .....                  | - 27 - |
| 3.5.4 Borba protiv fast-flux mreža.....           | - 28 - |
| 4. Budućnost Internet-a i DNS-a .....             | - 30 - |
| 4.1 ICANN i administracija DNS-a .....            | - 30 - |
| 4.2 Alternativni DNS.....                         | - 32 - |
| 4.3 Budućnost DNS-a.....                          | - 33 - |
| Zaključak .....                                   | - 34 - |
| Literatura.....                                   | - 35 - |

## Uvod

---

Sistem imenovanja domena (*Domain Name System* – DNS) je distribuirana baza podataka o hostovima na *Internet*-u. Njegov zadatak je prevodjenje naziva računara u IP adrese i obrnuto. Zbog važnosti ovih informacija, a naročito u poslednjim godinama, postoji snažna potreba za obezbeđivanjem komunikacije u okviru DNS sistema. Trenutni (nebezbedni) DNS ne sprečava napadače da modifikuju ili ubacuju DNS podatke, što im omogućava različite vrste zloupotreba.

Da bi se obezbedila njegova sigurnost, DNS je proširen ekstenzijama (DNSSec) koje funkcionišu na principu kriptografije javnog ključa. DNSSec je projektovan da zaštiti DNS od nekih pretnji, kao što je “trovanje keša” DNS-a (*cache poisoning*), ali ne i od svih (kao što je DDoS).

Sajber-kriminal je danas jedna od ozbiljnih globalnih pretnji, koja odnosi ogroman profit uz minimalni rizik za kriminalce, koji su motivisani da stalno unapređuju maliciozni softver. Možda najmoćnije oružje u rukama ovakvih pojedinaca ili grupa predstavljaju *bot* mreže, grupe kompromitovanih računara na kojima se izvršavaju programi, instalirani najčešće preko crva ili trojanaca, pod zajedničkom komandnom i kontrolnom infrastrukturom. Nova, sofisticirana tehnika rada ovakvih mreža, poznata kao *fast-flux*, se snažno oslanja na DNS, konstantno menjajući javne zapise svojih adresa da bi se sprečilo njihovo otkrivanje.

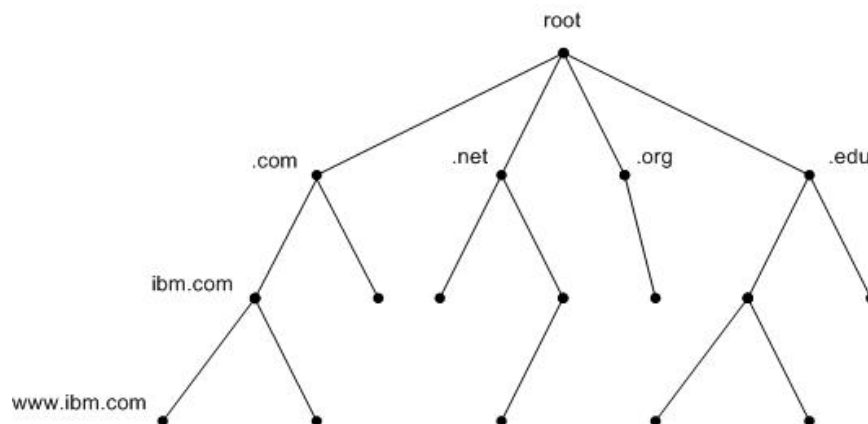
Da bi se maksimalno iskoristile prednosti obezbeđivanja DNS-a, kao i da bi najvažniji zadaci uvodjenja bezbednog DNS-a bili ispunjeni, neophodno je da kompletan DNS sistem bude obuhvaćen. Ovo sa sobom povlači mnoge probleme, od kojih je najveći i najvažniji obezbeđivanje DNS *root*-a i kontrola nad *root*-om koju to obezbeđivanje donosi.

## 1. Pregled DNS-a

### 1.1 Struktura DNS-a

DNS je globalna, hijerarhijska i distribuirana baza podataka. Ova baza podataka, koja se čuva na serverima naziva, povezuje kanonička imena, koja koristimo kao nazive domena, sa određenim podacima koji se nazivaju zapisi resursa (*Resource Records* – RRs). Zapisi koji se odnose na naziv domena mogu biti različitih tipova, ali je tip *adresa* najčešći. Skup zapisa resursa istog tipa se označava kao *Resource Record Set* (RRSet).

Pošto nazivi domena moraju da budu globalno jedinstveni, koristi se hijerarhijski princip davanja imena. Naziv domena se odnosi na jedan čvor u stablu koje nazivamo adresni prostor domena (*domain name space*). Ovo stablo naziva domena (slika 1.1) je vrlo slično fajl sistemu Windows ili Linux operativnog sistema. Svako podstablo se naziva domenom. Na primer, podstablo sa korenom u .com čvoru se naziva .com domenom i obuhvata sve nazive domena koji se završavaju sa .com. Čvorovi koji su direktni potomci (*child*) korenog čvora se nazivaju domeni najvišeg nivoa (*Top Level Domain* – TLD).

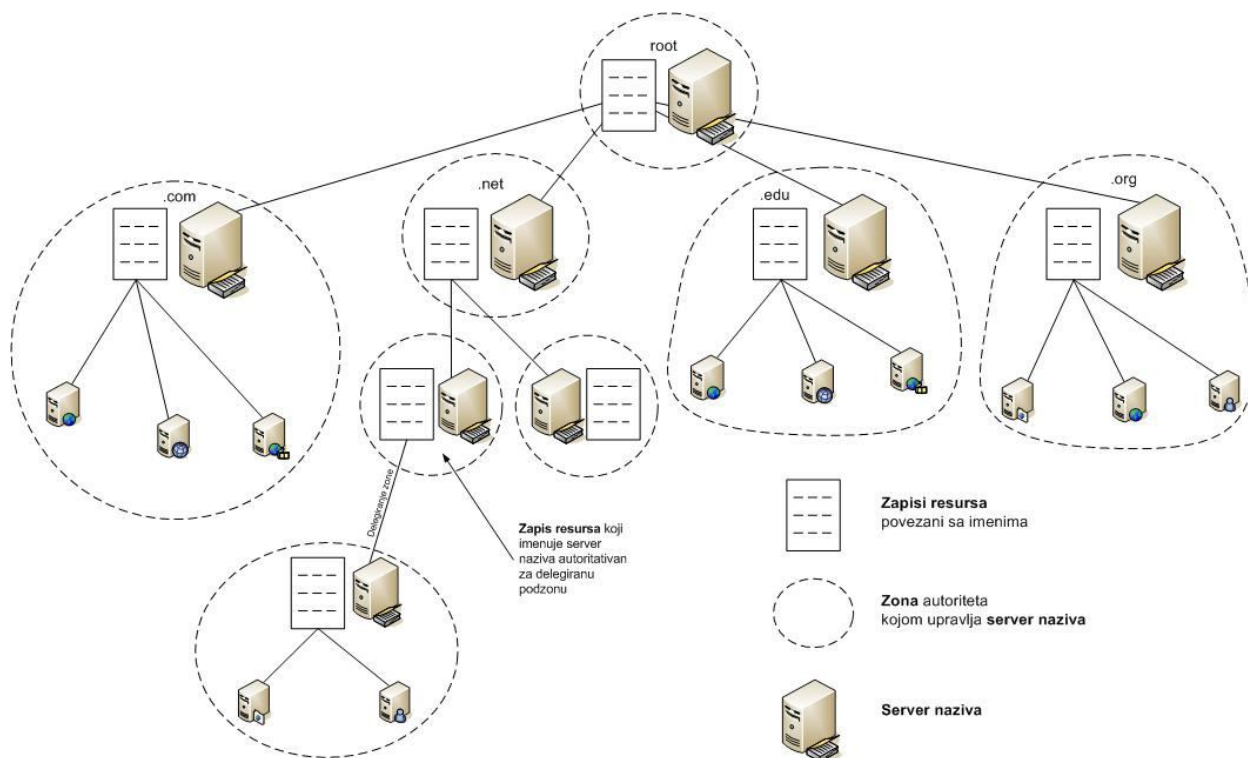


**Slika 1.1.** Stablo naziva domena

Komunikacija sa DNS bazom podataka prati klijent-server arhitekturu. Stablo naziva domena je podeljeno u zone, koje predstavljaju susedne delove stabla. Zone se određuju procesom delegiranja kojim se nekoj organizaciji daje odgovornost upravljanja pojedinim poddomenima. Zona može da sadrži informacije o domenima i njihovim poddomenima. Zone najvišeg nivoa, kao što je .edu, uglavnom sadrže informacije o delegiranju.

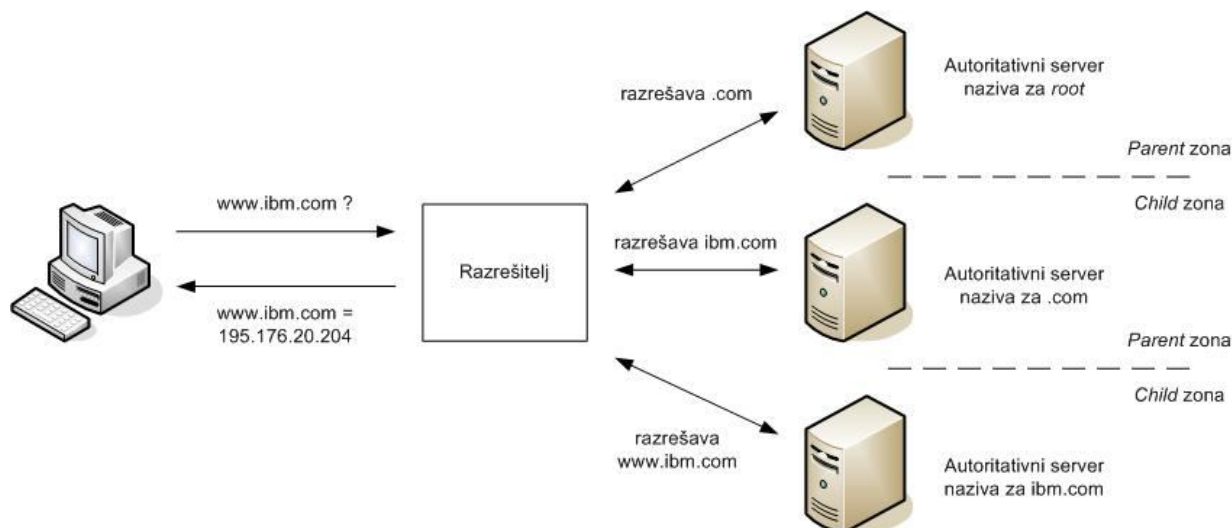
Za svaku zonu postoje autoritativni serveri (serveri naziva) koji odgovaraju na upite vezane za nazive domena u toj zoni. Serveri naziva mogu biti autoritativni i za više zona. Klijentski program za pristup DNS-u se naziva razrešitelj (*resolver*). Kada razrešitelj primi upit,

on ga prvo prosledjuje jednom od *root* DNS servera koji opslužuju *root* domen. Kao odgovor, dobija se sledeći server u nizu koji je “bliži” autoritativnom serveru iz traženog upita.



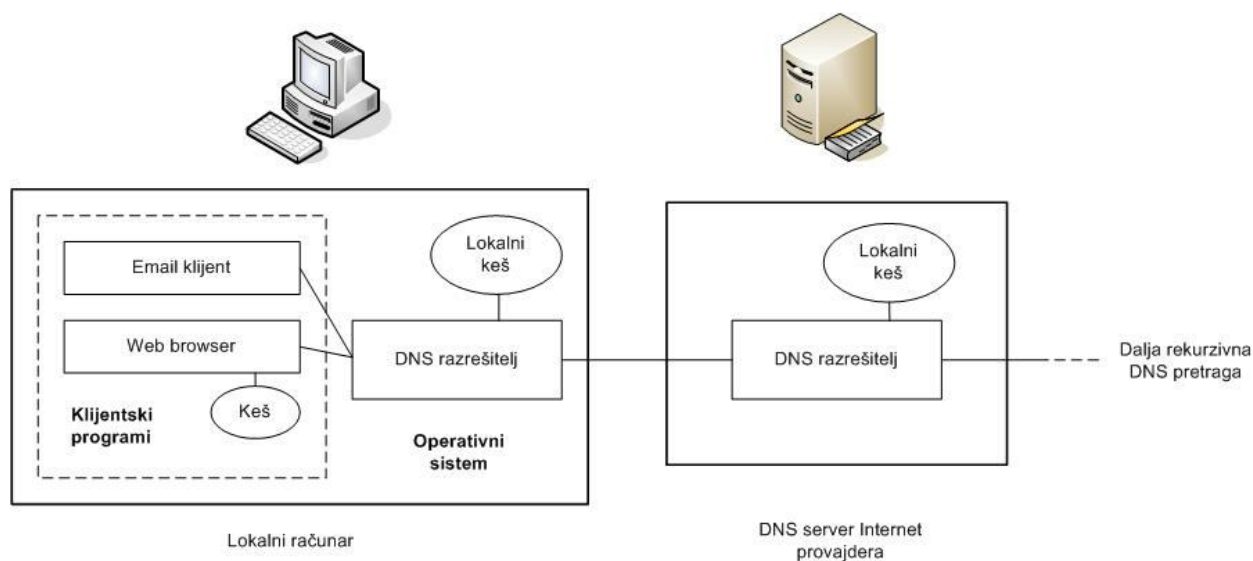
**Slika 1.2.** Adresni prostor domena

Na primeru na slici 1.3, razrešitelj prima upit za IP adresom za *www.ibm.com*. Razrešitelj potom prosledjuje upit *root* DNS serveru, koji kao odgovor vraća IP adresu DNS servera koji je autoritativan za *.com* zonu. Razrešitelj zatim šalje upit serveru naziva koji je autoritativan za *.com* i kao odgovor dobija IP adresu servera naziva autoritativnog za *ibm.com*. Konačno, kontaktira se DNS server za *ibm.com* koji šalje IP adresu za *www.ibm.com* za koju je i autoritativan. Ovaj odgovor se zatim vraća klijentu koji je poslao upit. Ovaj celokupni proces se naziva razrešavanje (*resolving*).



Slika 1.3. Razrešavanje DNS upita

Radi ubrzanja razrešivanja upita, kao i rasterećenja servera naziva na svim nivoima, koristi se tehnika keširanja rezultata upita, koji se čuvaju u memoriji određeno vreme.



Slika 1.4. Keširanje DNS podataka

*Root* serveri su od suštinskog značaja za funkcionisanje DNS sistema. Postoji 13 različitih *root* servera (slika 1.5) koji su, uz višestruku replikaciju, razmešteni po celom svetu. Uz njih, koriste se tehnike keširanja da bi se smanjio saobraćaj i broj zahteva kao i ubrzao proces razrešavanja. Kao posledica, svaki zapis resursa koji se dobije od DNS servera poseduje određeni životni vek (*time-to-live* – *TTL*) koji predstavlja vreme u kojem se taj zapis resursa može keširati.



**Slika 1.5.** Geografske lokacije svih *root* servera (Mart 2007). Izvor: RIPE NCC

## 1.2 Struktura DNS podataka

Da bi se razumeli bezbednosni problemi i rizici DNS-a, kao i moguća rešenja, mora se poznavati način funkcionisanja DNS protokola. Za to je potreban uvid u strukturu podataka koji se koriste u DNS-u.

Svi **zapisi resursa** u DNS-u imaju isti osnovni format:

|          |                                                               |
|----------|---------------------------------------------------------------|
| NAME     | Ime vlasnika, tj. naziv čvora na koji se odnosi zapis resursa |
| TYPE     | Tip zapisa resursa                                            |
| CLASS    | Šifra klase                                                   |
| TTL      | Vreme u sekundama za koje zapis resursa ostaje validan        |
| RDLENGTH | Dužina RDATA polja                                            |
| RDATA    | Ostali podaci specifični za svaki zapis resursa               |

Sva komunikacija u okviru DNS protokola ima isti format koji nazivamo **poruka**:

|            |                                                                 |
|------------|-----------------------------------------------------------------|
| HEADER     | Zaglavlje poruke                                                |
| QUESTION   | Pitanje za server naziva                                        |
| ANSWER     | Zapisi resursa koji odgovaraju na pitanje                       |
| AUTHORITY  | Zapisi resursa sa informacijama o autoritativnom serveru naziva |
| ADDITIONAL | Zapisi resursa koji sadrže dodatne informacije                  |

Deo za **pitanje** se koristi za prenos “pitanja” u većini upita, tj. parametara koji određuju šta se pita.

|        |                                                                |
|--------|----------------------------------------------------------------|
| QNAME  | Ime domena predstavljeno nizom oznaka                          |
| QTYPE  | Kod koji određuje tip upita                                    |
| QCLASS | Kod koji određuje klasu upita, na primer IN za <i>Internet</i> |

**Zaglavlje poruke** je uvek prisutno i određuje koja od preostalih polja su prisutna, da li je poruka upit ili odgovor itd.

| ID      |        |    |    |    |    |   |       |
|---------|--------|----|----|----|----|---|-------|
| QR      | Opcode | AA | TC | RD | RA | Z | RCODE |
| QDCOUNT |        |    |    |    |    |   |       |
| ANCOUNT |        |    |    |    |    |   |       |
| NSCOUNT |        |    |    |    |    |   |       |
| ARCOUNT |        |    |    |    |    |   |       |

|         |                                                                                                                                                                                      |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ID      | Identifikator koji postavlja program koji generiše bilo kakav upit. Ovaj identifikator se kopira u odgovarajući odgovor i može se koristiti za uparivanje odgovora na nerešene upite |
| QR      | Polje koje određuje da li je poruka upit ili odgovor                                                                                                                                 |
| Opcode  | Polje koje određuje vrstu upita u poruci. Postavlja ga pošiljalac upita; kopira se u odgovor                                                                                         |
| AA      | <i>Authoritative Answer</i> – polje validno u odgovorima, određuje da je server naziva koji odgovara autoritativan za domen u polju QUESTION                                         |
| TC      | <i>TrunCation</i> – ukazuje da je poruka skraćena usled dužine veće od maksimalno dozvoljene na prenosnom kanalu                                                                     |
| RD      | <i>Recursion Desired</i> – ovo polje može biti postavljeno u upitu i kopira se u odgovor. Ako je postavljeno, upućuje server naziva da vrši rekurzivni upit.                         |
| RA      | <i>Recursion Available</i> – polje se postavlja ili briše u odgovoru, označavajući da li je rekurzivan upit na serveru podržan ili ne                                                |
| Z       | Rezervisano za buduću upotrebu, mora biti prazno                                                                                                                                     |
| RCODE   | <i>Response Code</i> – Postavlja se kao deo odgovora, vraća se prazno/sa šifrom greške                                                                                               |
| QDCOUNT | Označava broj unosa u delu za pitanje                                                                                                                                                |
| ANCOUNT | Označava broj zapisa resursa u delu za odgovor                                                                                                                                       |
| NSCOUNT | Označava broj zapisa resursa na serveru naziva u delu za zapise o autoritativnosti                                                                                                   |
| ARCOUNT | Označava broj zapisa resursa u delu za dodatne zapise                                                                                                                                |

## 2. Mehanizmi za obezbedjenje DNS-a

---

### 2.1 DNSsec

DNSsec je predloženi standard koji modifikuje zapise resursa i protokole DNS-a da bi se obezbedila sigurnost za transakcije između razrešitelja i servera naziva. Uvođenjem podataka koji su kriptografski potpisani javnim ključem u DNS uz pomoć četiri nova zapisa resursa, DNSsec obezbeđuje:

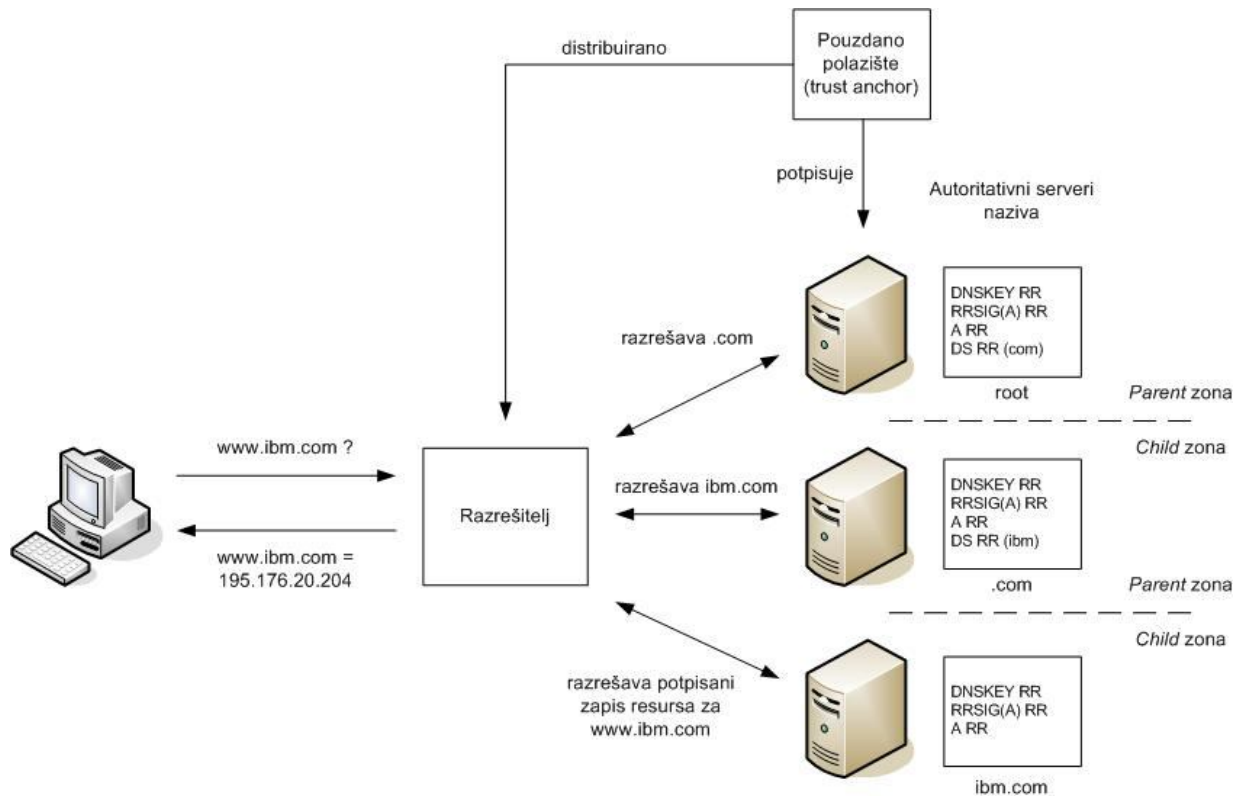
- Autentičnost izvora: Razrešitelj može da odredi da li odgovor potiče od autoritativnog servera naziva određene zone.
- Verifikaciju integriteta: Razrešitelj može da odredi da li je odgovor menjan u toku prenosa.
- Autentično poricanje postojanja: Razrešitelj može da potvrdi da je određeni upit nerazrešiv, ako ne postoji zapis resursa DNS-a na autoritativnom serveru naziva.

#### 2.2.1 Funkcionisanje DNSsec-a

DNSsec je osmišljen da zaštiti razrešitelje od lažiranih DNS podataka, kao što je slučaj pri “trovanju” DNS keša. Svi odgovori u DNSsec-u koji se šalju su digitalno potpisani. Proverom digitalnih potpisa, razrešitelj može da proveri da li je primljena informacija identična (tačna i kompletna) kao informacija na autoritativnom serveru naziva.

DNSsec uvodi četiri nova tipa zapisa resursa: Potpis zapisa resursa (RRSIG), DNS Javni ključ (DNSKEY), Potpisnik delegiranja (DS) i Sledeći bezbedan (NSEC).

DNSsec Server naziva za određenu zonu drži Potpis zapisa resursa (RRSIG) za različite skupove zapisa resursa (RRset) koje se na njemu drže. RRSIG predstavlja digitalni potpis koji se formira uzimanjem *hash*-a određenog skupa zapisa resursa u zoni i njegovom enkripcijom uz pomoć privatnog ključa iz kompleta kriptografskih ključeva administratora te zone. Odgovarajući javni ključ iz ovog kompleta se čuva u zapisu DNSKEY. Po primanju potpisanog DNS odgovora od servera naziva, DNSsec razrešitelj dešifruje RRSIG uz pomoću javnog ključa zone. Razrešitelj zatim generiše *hash* RRset dela odgovora i upoređuje ga sa *hash*-om dobijenim iz RRSIG dela odgovora. Na taj način se potvrđuje ili negira integritet i autentičnost porekla različitih tipova informacija.



Slika 2.1. DNSsec upit i odgovori

Kako razrešitelj dolazi do autentičnog DNSKEY ključa za određenu zonu? Zapis resursa Potpisnik delegiranja (DS) se obezbeđuje od strane *parent* zone i predstavlja tačku delegiranja između *parent* i *child* zona koja se može autentifikovati. Da bi potvrdio DNSKEY *child* zone, razrešitelj preuzima odgovarajući DS, RRSIG(DS) i DNSKEY *parent* zone. DS se verifikuje pomoću dešifrovanog RRSIG(DS) i zatim se DS podaci koriste za autentifikaciju DNSKEY podatka *child* zone. Na ovaj način, potpisani DS funkcioniše kao “sertifikat” koji se autoritativno isporučuje iz *parent* zone i vezuje *child* zonu za svoj DNSKEY. Server naziva iz *parent* zone postaje, praktično, “pouzdana treće lice”, koje olakšava razmenu DNS informacija između razrešitelja i *child* zone. Niz ovakvih delegiranih odnosa formira lanac autentifikacije, koji predstavlja putanju koju razrešitelj može da prati od javnog ključa (tj. pouzdanog polazišta – *trust anchor*) DNS *root*-a. Na kraju, Sledeći bezbedan (NSEC) zapis resursa povezuje potpisane resurse, omogućavajući razrešitelju da pretražuje fajl zone i da odredi da li određeni domen postoji u DNS-u.

## 2.2.2 Slabosti DNSsec-a

DNSsec nosi sa sobom nekoliko problema:

- DNSsec je kompleksan za uvođenje i u nekim slučajevima na granicama zona zahteva vrlo pažljiva podešavanja. Iskustva iz eksperimenata sugerišu da trivijalne greške u konfigurisanju zone ili ključevi koji su prestali da važe mogu izazvati ozbiljne probleme za DNSsec razrešitelj, i da mogućnosti trenutnog protokola da izveštava o greškama nisu adekvatne.

- DNSsec značajno povećava veličinu DNS paketa u odgovoru; izmedju drugih stvari, ovo čini DNSsec DNS servere još efektivnijim kao DoS amplifikatore.
- Provera odgovora DNSsec-a povećava opterećenje razrešitelja, jer DNSsec razrešitelj treba da izvrši validaciju potpisa i u nekim slučajevima treba da pošalje dodatne upite. Ovo povećanje opterećenja povećava i vreme potrebno da se pošalje odgovor originalnom DNS klijentu, što u nekim slučajevima može da dovede do *timeout*-a i ponovnog slanja upita. Štaviše, mnogi trenutni DNS klijenti su već isuviše nestrpljivi i bez dodatnih kašnjenja koje bi uveo DNSsec.
- Kao i sam DNS, model poverenja DNSsec-a je skoro potpuno hijerarhijski. Dok DNSsec dozvoljava razrešiteljima da saznaju javne ključeve van grupe onih koji se odnose na *root*, *root* ključ je onaj koji je zaista važan. Stoga bi bilo kakav kompromis u bilo kojoj zoni izmedju *root*-a i određenog naziva mogao da naruši sposobnost DNSsec-a da zaštiti integritet podataka vlasnika naziva. Ovo nije nikakva promena, jer nebezbedni DNS koristi isti model.
- Prelaz izmedju ključeva na *root*-u je vrlo težak. Ovaj problem do sada nije adekvatno rešen.
- DNSsec ima specifične zahteve za vremensku sinhronizaciju izmedju razrešitelja koji proverava i strane koja vrši DNSsec potpisivanje. Pre DNSsec-a, svi postupci povezani sa vremenom u DNS-u su mogli biti obavljani od strane mašine koje je radila samo sa “proteklom” ili “relativnim” vremenom. Zbog toga što je period validnosti DNSsec potpisa baziran na “apsolutnom” vremenu, razrešitelj koji proverava mora koristiti isti koncept apsolutnog vremena kao i potpisnik zone, da bi se odredilo da li je potpis u okviru svog perioda validnosti ili je istekao. Napadač koji može da promeni razrešiteljevo poimanje apsolutnog vremena može da ga prevari koristeći potpise koji su istekli. Takodje, napadač koji može da promeni poimanje trenutnog apsolutnog vremena potpisnika zone, može da prevari potpisnika zone na taj način da generiše potpise čiji se period validnosti ne poklapa sa onim što je potpisnik nameravao.

### 3. Bezbednosni problemi DNS-a

---

Po svojoj prirodi, DNS je javni sistem, što ga čini vrlo privlačnim za zlonamerne korisnike *Internet*-a. Postoji više aspekata kroz kojih se bezbednost DNS-a može posmatrati, od relativno jednostavnih do veoma kompleksnih. Da bi shvatili napade kojima je ovaj sistem svakodnevno izložen, moramo identifikovati sve aspekte sistema koje takvim korisnicima mogu poslužiti kao potencijalne tačke pristupa. Oni se suštinski mogu modeliti u četiri grupe:

- Administrativna bezbednost: Tiče se fizičke bezbednosti, dozvola za pristup fajlovima, konfiguracije servera, podešavanja DNS softvera (najčešće BIND-a) i sl. Administrativna bezbednost predstavlja osnovu odbrane sistema. Nijedna kriptografska tehnika ne vredi ako je osnovni sistem nestabilan ili dozvoljava neograničen pristup interesantnim fajlovima.
- Transferi zone: Predstavlja jedan od mehanizama koji administratorima omogućavaju repliciranje baze podataka sa DNS podacima. Transferi zone imaju nekoliko potencijalnih bezbednosnih problema, ali se oni lako rešavaju pravilnim podešavanjem DNS softvera.
- Dinamičko ažuriranje: Izlaže *master* fajl zone mogućem oštećenju, uništenju ili trovanju. Predostrožnosti u ovoj proceduri obuhvataju dobro projektovanje sistema, parametri DNS softvera (najčešće BIND-a), zaštitne barijere (*firewall*) i autentifikacija.
- Integritet zone: Ako je neophodno da podaci u zoni koju koristi DNS ili krajnji host budu apsolutno ispravni (tj. da odgovori na upite nisu menjani i da podaci koji se vraćaju zaista potiču od vlasnika zone), mora se koristiti DNSsec. DNSsec je predmet važnih eksperimenata i naknadnih promena u poslednjih četiri ili pet godina. Njegova druga generacija, pominjana i kao *DNSsec.bis*, predstavlja rezultat zajedničkog truda IETF<sup>1</sup>-a, *root* server operatera kao i regionalnih *Internet* registara.

Bezbednost DNS-a se može posmatrati i kroz konkretne pretnje. Postoji nekoliko različitih klasa pretnji po DNS, od kojih su većina slučajevi opštih problema reflektovani na DNS, ali su neke specifične za osobenosti njegovih protokola.

---

<sup>1</sup> *Internet Engineering Task Force*. Razvija i promoviše *Internet* standarde, blisko saradjujući sa W3C i ISO/IEC.

### 3.1 DNS lažiranje

Lažiranje DNS podataka predstavlja promenu mapiranja naziva nekog domena sa legitimne IP adrese na adresu koju odabere napadač.

Opšti oblik lažiranja izgleda ovako:

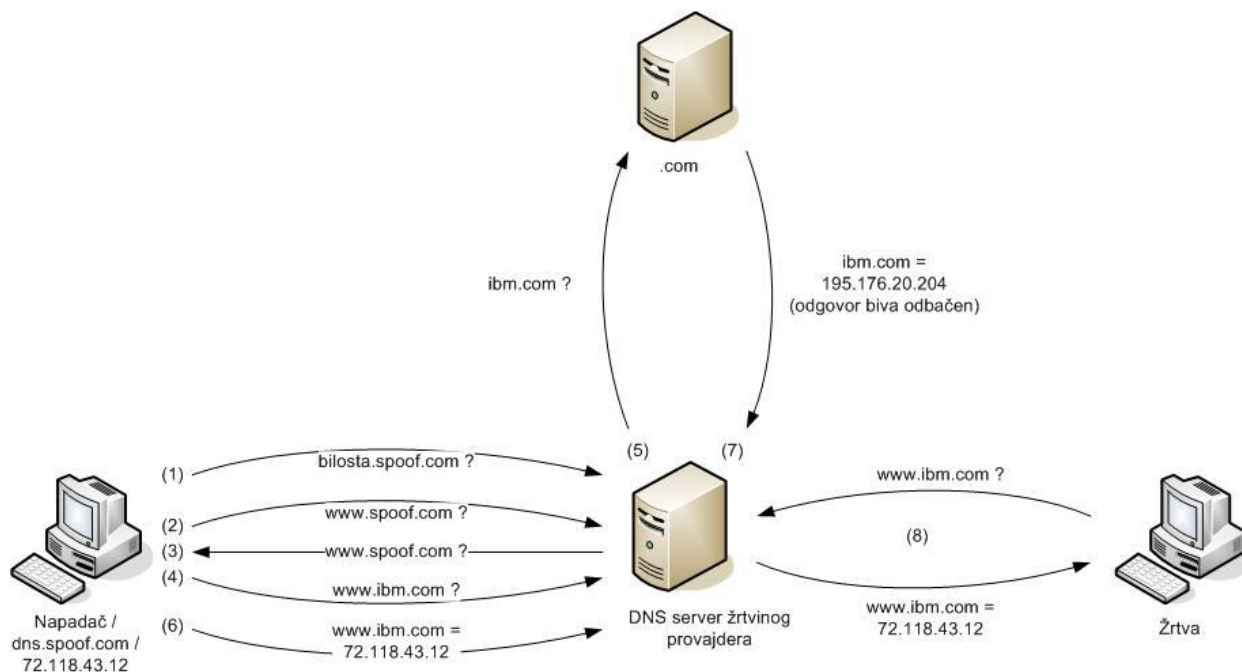
- Žrtva šalje upit, možda i na podsticaj od strane napadača ili neke treće strane; u nekim slučajevima sam upit može biti nepovezan sa nazivom koji se napada (tj. napadač samo koristi ovaj upit kao način da ubaci lažne informacije o nekom drugom nazivu).
- Napadač ubacuje odgovor, bilo putem presretanja paketa, pogadjanja upita ili time što je legitimni server naziva koji je u nekom trenutku uključen u proces odgovaranja na upit koji je žrtva poslala.
- Napadačev odgovor sadrži jedan ili više zapisa resursa sa DNS nazivima u polju RDATA; u zavisnosti od toga kog je određenog oblika ovaj napad, cilj može biti da se ubace lažni podaci povezani sa tim nazivima u keš žrtve preko *Additional* dela ovog odgovora ili da se sledeća faza upita preusmeri na server koji određuje napadač (da bi se ubacili kompleksniji lažni podaci u žrtvin keš a koji mogu lako da stanu u jedan odgovor ili da bi se lažni podaci ubacili u *Authority* ili *Answer* delove odgovora gde će imati veće šanse da prevare razrešitelj).

Detaljan prikaz mogućeg scenarija DNS lažiranja dat je na slici 3.1. Napadač može da natera DNS server žrtvinog provajdera da pošalje zahtev za traženje adrese *www.ibm.com*. Zbog korišćenja UDP protokola, DNS server ne može da potvrdi od koga je dobio odgovor. Napadač to može da iskoristi falsifikujući očekivani odgovor i da tako ubaci drugu IP adresu u keš DNS servera.

Važno je napomenuti da svaki zahtev nosi redni broj, na osnovu koga server povezuje odgovore sa zahtevima. Da bi saznao tekući redni broj, on može da registruje domen *spoof.com*, sa adresom *72.118.43.12*. Za svoj domen napadač pravi i DNS server *dns.spoof.com*, koji ima istu adresu s obzirom da se radi o istoj napadačevoj mašini.

Prvi korak je da se od žrtvinog servera naziva traži adresa računara *bilosta.spoof.com* (1), što će kao rezultat dovesti do slanja upita autoritativnom serveru naziva za *.com* i unošenja napadačevog DNS servera u keš, kao autoritativnog za taj domen. Napadač zatim od servera naziva provajdera traži adresu *www.spoof.com* (2). Server naziva provajdera taj zahtev, naravno, šalje napadačevom DNS serveru (3). Taj zahtev nosi redni broj koji je napadaču potreban. Sledećeg trenutka, napadač šalje nov zahtev, ovaj put za *www.ibm.com* (4) i istog trenutka odgovara na sopstveni zahtev, šaljući serveru naziva falsifikovani odgovor (6) u ime servera autoritativnog za *.com*: *www.ibm.com = 72.118.43.12*. Taj falsifikovani odgovor nosi redni broj za jedan veći od broja koji je prethodno primljen. Iako je provajderov server naziva u međuvremenu poslao upit serveru naziva autoritativnog za *.com* (5), napadačev odgovor sa ispravnim rednim brojem će stići pre njegovog odgovora, i napadačev odgovor biva keširan, dok pravi odgovor biva odbačen (7) kao netražen.

Na kraju, kada odabrana žrtva ili bilo ko drugi ko u tom trenutku koristi server naziva istog provajdera zatraži adresu lokacije *www.ibm.com* (8), biće usmeren na napadačevu mašinu, gde ih može dočekati lažni *web* server.



Slika 3.1. DNS lažiranje

Zajedničko za sve napade lažiranjem je da poruke odgovora dozvoljavaju napadaču da unese proizvoljne DNS nazive i da obezbedi dodatne informacije za koje napadač tvrdi da su povezane sa ovim nazivima; izuzev ako žrtva zna prave podatke koji su vezani za ove nazive, biće vrlo teško odbraniti se od ovakvog napada.

Ova vrsta napada je naročito podmukla s obzirom na to da je napadaču vrlo lako da isprovocira žrtvu da pošalje upit za određeni naziv po napadačevom nahodjenju, na primer postavljanjem linka u grafiku veličine 1x1 piksela (*web bug*<sup>2</sup>) koja je deo Text/HTML *email* poruke upućene žrtvi. Ako žrtvin program za čitanje pošte pokuša da prati taj link, rezultat će biti DNS upit za naziv koji je odabrao napadač.

DNSsec obezbedjuje dobru odbranu od većine varijacija ove klase napada. Proveravanjem potpisa, razrešitelj može da odredi da li su podaci vezani za neki naziv zaista uneseni od strane delegiranog autoriteta za taj deo DNS adresnog prostora. Preciznije, razrešitelj može da odredi da li je strana koja je unela podatke imala pristup navodno tajnom ključu čiji se odgovarajući javni ključ pojavljuje na očekivanoj lokaciji u DNS adresnom prostoru sa očekivanim lancem *parent* potpisa koji počinju javnim ključem koji razrešitelj već poznaje.

DNSsec potpisi ne pokrivaju *glue*<sup>3</sup> zapise, tako da i dalje postoji mogućnost napada lažiranjem koji obuhvata *glue*, ali uz pomoć DNSsec-a je moguće otkriti ovaj napad privremeno prihvatajući *glue* da bi se preuzele potpisane autoritativne verzije istih podataka i provere njihovih potpisa.

<sup>2</sup> Objekat koji se postavlja u *web* stranu ili *email* poruku, obično nevidljiv za korisnika, koji pokreće neki zahtev za dohvaćanje sa *Internet*-a i time, neizbežno, slanje DNS upita.

<sup>3</sup> Serveri naziva se u delegiranjima pojavljuju u formi naziva, a ne u formi IP adrese. Ovo znači da razrešitelj mora da pošalje još jedan DNS zahtev da bi saznao IP adresu servera na koji je upućen. Pošto ovo može da dovede do kružne zavisnosti (*circular dependency*) ako je server naziva na koji se upućuje ispod domena za koji je autoritativan, povremeno je neophodno da server naziva koji delegira obezbedi i IP adresu narednog servera naziva. Ovaj zapis se naziva *glue* zapis.

### 3.2 Prevara od strane servera kome se veruje

Još jedna varijacija napada presretanjem paketa je poverljivi server za koji se ispostavi da nije takav, bilo slučajno ili namerno. Mnoge klijentske mašine su konfigurisane tako da koriste samo servere kojima veruju da u njihovo ime vrše DNS upite. U mnogo slučajeva, ovi poverljivi serveri se održavaju od strane korisnikovog provajdera, i oglašavaju se klijentima preko DHCP-a ili PPP opcije. Osim slučajne “prevare” ovog poverljivog odnosa (usled grešaka na serveru, uspešnih provala u server, i sl.), sam server može biti konfigurisan tako da vraća odgovore koji nisu ono što korisnik očekuje, bilo u iskrenom pokušaju da pomogne korisniku ili u neke druge svrhe kao što je unapređjivanje partnerstva između provajder i neke treće strane.

Ovaj problem je naročito izražen za česte putnike, koji nose sopstvenu opremu i očekuju da ona radi na isti način gde god da dodju. Ovakvim putnicima je potreban DNS kojem mogu da veruju bez obzira ko drži mrežu u koju je njihova oprema trenutno povezana ili koje su marke uredjaji koje lokalna infrastruktura koristi.

Dok bi očigledno rešenje ovog problema bilo da klijent koristi server u koji ima poverenja, u praksi klijent ne mora da ima ovu mogućnost. U mnogim mrežnim okruženjima, klijentska mašina ima ograničen skup servera naziva koje može da odabere, od kojih ni u jednog ne mora da ima poverenja. U ekstremnim slučajevima, filterisanje portova ili drugi oblik presretanja paketa može sprečavati klijenta da pokrene iterativni<sup>4</sup> razrešitelj čak iako je vlasnik klijentske mašine voljan i sposoban da to uradi. Stoga, iako uzrok ovog problema nije napad na DNS protokol, ovakva vrsta “prevare” je pretnja za DNS klijente i jednostavno prebacivanje na neki drugi rekurzivni<sup>5</sup> server naziva nije adekvatna odbrana.

Posmatrano sa mesta DNS protokola, u ovom slučaju klijent dobrovoljno šalje zahtev napadaču i razrešitelj mora samostalno da proveri DNSsec potpise da bi autentifikovao server kojem želi da veruje.

Neobičan primer “prevare” servera kome se podrazumevano veruje predstavlja kontroverzna taktika za borbu protiv *bot* mreža koju neki američki provajderi povremeno koriste već nekoliko godina unazad.

*Cox Communication* je jula 2007. počeo sa presretanjem pokušaja da se kontaktiraju određeni *online chat* kanali i preusmeravao ih ka serveru koji je pokušavao da sa korisničkih računare ukloni *spyware*. Ovime je kompanija pokušala da očisti računare od zlonamernih programa koji preuzimaju kontrolu nad resursima računara, u svrhe slanja neželjene pošte ili učestvovanja u različitim mrežnim napadima, kao deo velike mreže kompromitovanih računara poznatih kao *bot* mreže.

Konkretno, DNS server provajdera Cox je na zahtev za adresom domena pojedinih IRC servera, umesto njihovom pravom adresom, odgovarao IP adresom sopstvenog IRC servera (70.168.70.4)<sup>6</sup>.

<sup>4</sup> Iterativni DNS upit/server obezbeđuje delimičan odgovor, usmeravanje na neki drugi server naziva ili vraća grešku. DNS serveri moraju podržavati ovakve upite.

<sup>5</sup> Rekurzivni DNS upit/server obezbeđuje potpuni odgovor ili vraća grešku, bez mogućnosti upućivanja na neki drugi server naziva. Serveri naziva ne moraju da podržavaju ovakav režim rada.

<sup>6</sup> <http://www.exstatica.net/hijacked/>

prave IP adrese *mzima.net* IRC mreže:

```
;; QUESTION SECTION:
;irc.mzima.net. IN A

;; ANSWER SECTION:
irc.mzima.net. 43200 IN A 216.193.223.223
```

zapis iz *Cox*-ovog servera naziva *ns1.dc.cox.net*:

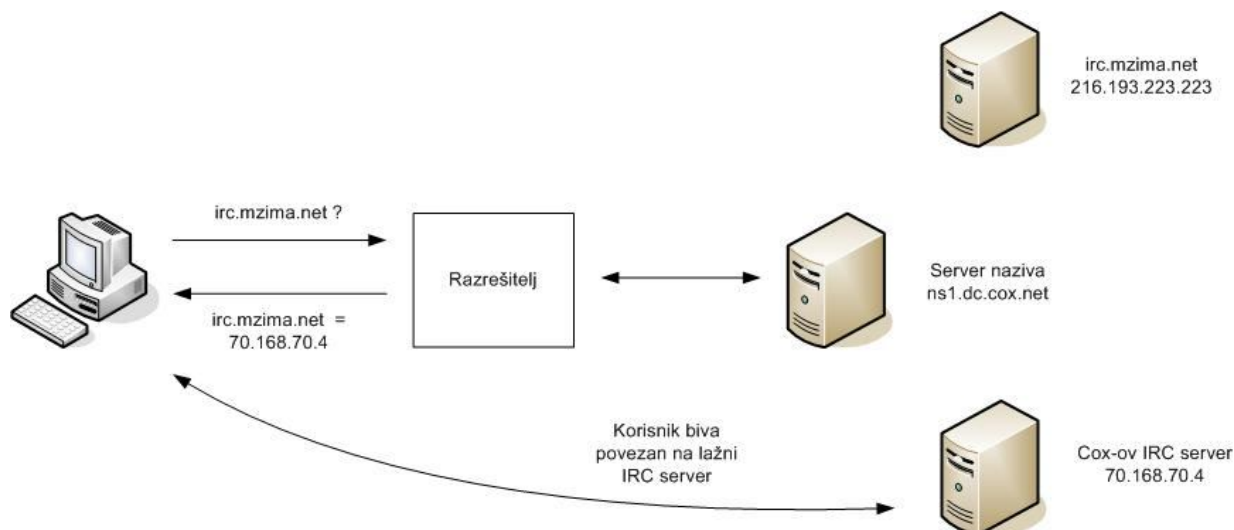
```
;; QUESTION SECTION:
;irc.mzima.net. IN A

;; ANSWER SECTION:
irc.mzima.net. 300 IN A 70.168.70.4
```

Po povezivanju, taj server je korisničkom računaru slao komande koje bi se izvršavale u pokušaju da se zlonamerni programi uklone:

```
#martian_
[INFO] Channel view for "#martian_" opened.
-->| YOU (andrew.m) have joined #martian_
== Mode #martian_ +nt by localhost.localdomain
== Topic for #martian_ is ".bot.remove"
== Topic for #martian_ was set by Marvin_ on Sunday, July 22, 2007 2:55:02 PM
== Topic for #martian_ is ".remove"
== Topic for #martian_ was set by Marvin_ on Sunday, July 22, 2007 2:55:02 PM
== Topic for #martian_ is ".uninstall"
== Topic for #martian_ was set by Marvin_ on Sunday, July 22, 2007 2:55:02 PM
== Topic for #martian_ is "!bot.remove"
== Topic for #martian_ was set by Marvin_ on Sunday, July 22, 2007 2:55:02 PM
== Topic for #martian_ is "!remove"
== Topic for #martian_ was set by Marvin_ on Sunday, July 22, 2007 2:55:02 PM
== Topic for #martian_ is "!uninstall"
== Topic for #martian_ was set by Marvin_ on Sunday, July 22, 2007 2:55:02 PM
<Marvin_> .bot.remove
<Marvin_> .remove
<Marvin_> .uninstall
<Marvin_> !bot.remove
<Marvin_> !remove
```

Ovaj slučaj, kao i prethodni njemu slični, je izazvao dosta pažnje i negativnih komentara jer, iako je predstavljao pokušaj uklanjanja zlonamernih programa sa računara, u suštini poseduje sve karakteristike *man in the middle* napada. Cox je pratio saobraćaj usmeren od svojih korisnika ka određenim adresama i presretao ga, usmeravajući korisnike na alternativnu adresu i potom izvršavajući naredbe na računarima korisnika – bez ikakvog objašnjenja ili upozorenja.



**Slika 3.2.** Preusmeravanje korisnika na Cox-ov IRC server

Iako je sa tehničke strane ovaj čin bio ispravan i dobronameran, sa legalne strane je u najboljem slučaju bio sumnjiv. Koncept same ideje je bio dobar ali, na kraju, gotovo je sigurno da su efekti koje je imao bili zanemarljivi i da nisu obuhvatili veći broj zaraženih računara. Postoji veliki broj *bot*-ova koji su jedinstveni. Mnogi čak zahtevaju specifične informacije o vlasniku *bot* mreže, tj. komplet komandi *bot*-a je najčešće jedinstven. Takođe, napredne tehnike, kao što je *fast flux*, koje se danas sve češće koriste, vrlo lako zaobilaze ovakvu taktiku.

Medjutim, bez obzira na namere i rezultate ove akcije, ona pokazuje na koji se način može zloupotrebiti poverenje poklonjeno neobezbedjenom DNS serveru.

### 3.3 Napad radi blokiranja usluga

Napad radi blokiranja usluga (*Denial of Service – DoS*) napad je pokušaj da se neki resurs učini nedostupnim korisnicima kojima je namenjen. Iako se načini, motivi i mete za DoS napad mogu razlikovati, obično se sastoji od uskladjених i zlonamernih napora jedne osobe ili više njih, da se neki *Internet* sajt ili servis spreči da funkcioniše efikasno ili da ne funkcioniše uopšte, privremeno ili trajno.

Izvršioci DoS napada obično, mada ne ekskluzivno, ciljaju sajtove ili servise koji su hostovani na visokopofilnim *web* serverima. Zajednički metod za ovu vrstu napada predstavlja obasipanje mete (žrtve) spoljnim zahtevima, tako da ne može da odgovori na legitimni saobraćaj, ili da odgovara toliko sporo da efektivno bude nedostupna. DoS napadi se ostvaruju putem:

- Prisiljavanjem računara koji su meta da se restartuju ili da zauzmu sopstvene resurse u tolikoj meri da ne mogu da obezbede uslugu za koju su namenjeni, ili
- Ometanjem komunikacionog medijuma između korisnika kojima je namenjen i žrtve tako da nisu u stanju da adekvatno komuniciraju.

Kao i svaki mrežni servis (kao i skoro svaki servis bilo koje vrste iz bilo kog domena o kome je reč) DNS je podložan DoS napadima. DNSsec ne može da bude od pomoći, čak može i

da pogorša problem za razrešitelje koji proveravaju potpise, jer provera potpisa povećava troškove procesiranja po DNS poruci a u nekim slučajevima može i da poveća broj poruka neophodan za odgovor na upit.

DNS serveri su takodje pod rizikom da budu iskorišćeni kao pojačavači DoS napada, jer su DNS paketi koji se šalju kao odgovor obično značajno veći od paketa DNS upita. DNSsec ne može da pomogne u rešavanju ovog problema.

DoS napadi se danas najčešće koriste u svojoj distribuiranoj varijanti – DDoS.

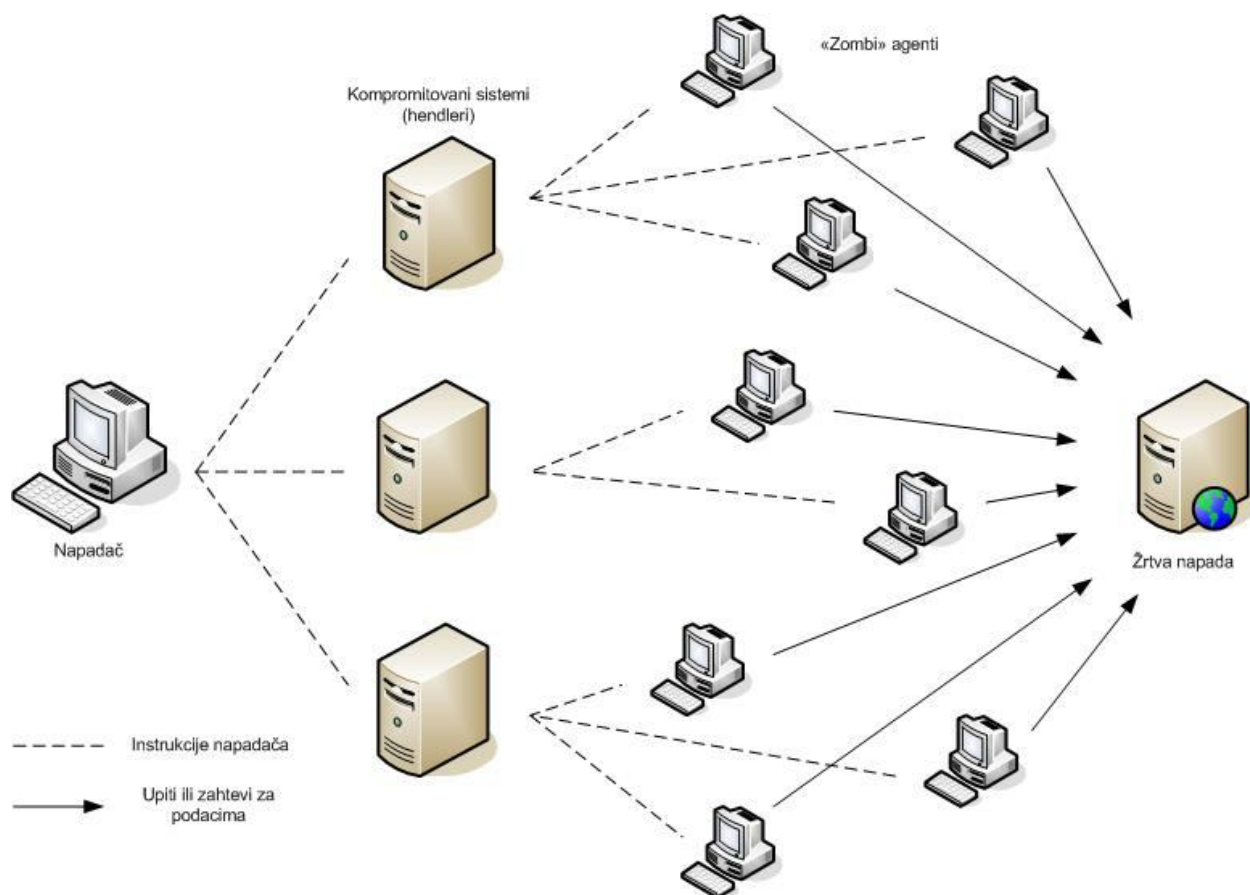
Distribuirani DoS (DDoS) napad se pokreće kada veći broj kompromitovanih sistema obasipa propusnu moć ili resurse ciljanog sistema. Ovi sistemi se kompromituju od strane napadača korišćenjem različitih metoda.

### 3.4 Bot mreže

Glavna prednost korišćenja DDoS napada za napadače je što veliki broj mašina može da stvori mnogo više saobraćaja od jedne mašine, što je mnogo teže isključiti veći broj mašina koje napadaju i što ponašanje svake mašine može biti prikrivenije, što je čini mnogo težom za lociranje i isključenje. Kupovina većeg propusnog opsega jednostavno ne funkcioniše, jer napadač može lako da poveća broj mašina koje napadaju.

Zlonamerni programi mogu da nose u sebi DDoS mehanizme, kao što je bio slučaj sa *MyDoom* kompjuterskim crvom. Sistemi se takodje mogu kompromitovati trojancem, koji dozvoljava napadaču da ubaci u sistem „zombi agenta“ (mada i sam trojanac može da ga sadrži).

Najstariji primer DDoS softvera je *Stacheldraht*. On koristi slojevitou strukturu u kojoj napadač koristi klijentski program da bi se povezao sa handlerima, koji su u stvari kompromitovani sistemi koji služe za izdavanje komandi „zombi agentima“ koji izvršavaju DDoS napad. Agenti se kompromituju preko handlera, korišćenjem automatizovanih rutina za iskorišćavanje slabosti u programima koji se koriste na mašinama žrtava. Svaki handler može da kontroliše do hiljadu agenata, pa ukupan broj mašina u službi napadača može da dostigne stotine hiljada. Ovakvi skupovi kompromitovanih sistema poznati su pod imenom *bot mreže*.



Slika 3.3. Korišćenje bot mreže za DDoS napad

Bot mreže obično koriste besplatne DNS hosting servise kao što su *DynDns.com*, *No-IP.com* ili *Afraid.org* da bi usmerili svoj poddomen prema IRC serveru koji kontroliše botove. Dok ovi besplatni DNS servisi ne služe kao izvor napada, oni obezbeđuju referentne tačke, često trajno upisane u izvršni program bot mreže. Uklanjanje ovakvih usluga obično onemogućava celokupnu bot mrežu. U skorije vreme, navedene kompanije su preduzele mere za čišćenje od ovakvih poddomena, usmeravajući ovakve poddomene na nedostupne IP adrese.

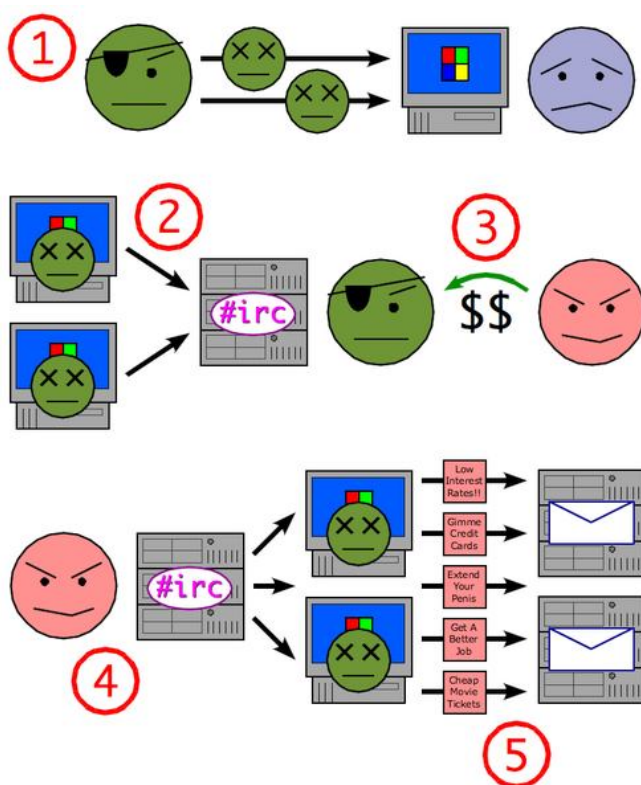
```

[+mnstj]: Hammer/Cable/Inferno: I have to well done to everyone eh.. we have a total o...
<Electron> !d# [mnstj]: Hammer/Cable/Inferno: I have to well done to everyone eh.. we have a total of 350 bots now (if
<Electron> -showstats
<BotMonitor> If all bots were online we would have: 375 bots.
This would equal: 6392KB/Sec of BandWidth
<Electron> you better ph34r
<Electron> can you login to them
<Electron> ?
<Electron> !login M_/0Z_/0ZM+.R]07T]07TR<C^T^+H\ +QGN6<Y^;ER]#1Y./B
U]K9S,0* [>SK807[DX^*>Y9S#PL'S\0'U]?2TL[+AX-]%'
<Electron> !udppacket 5000 207.71.92.193 80
<Electron> !udppacket stop
<Electron> !udppacket stop
<Electron> !udppacket stop
<Electron> !udppacket stop
<Electron> !udppacket stop
<Electron> -showstats
<BotMonitor> If all bots were online we would have: 377 bots.
This would equal: 6426KB/Sec of BandWidth
  
```

Slika 3.4. Komandna soba bot mreže na IRC serveru

Životni ciklus bot mreža najčešće izgleda ovako:

1. Napadač šalje viruse ili crve sa *bot* aplikacijom, koji inficiraju korisničke računare.
2. *Bot* na korisničkom računaru se povezuje na određeni IRC server (ponekad i *web* server). Ovakvi serveri se nazivaju serveri komande i kontrole.
3. Spamer kupuje pristup *bot* mreži od napadača.
4. Spamer zatim šalje instrukcije inficiranim računarima preko komandnog IRC servera...
5. ...naredjujući im da šalju neželjenu poštu *mail* serverima



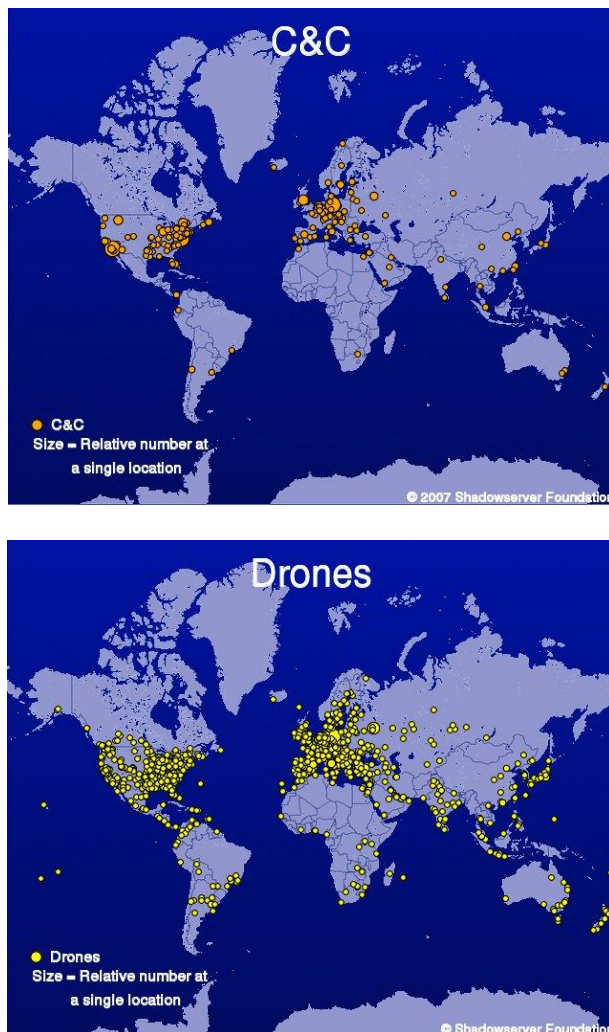
**Slika 3.5.** Korišćenje *bot* mreže za slanje neželjene elektronske pošte

Za razliku od *MyDoom* crva, koji je u sebi nosio upisanu samo jednu IP adresu protiv koje je napad bio usmeren, *bot* mreže mogu biti usmerene protiv bilo koje IP adrese. Sofisticirani napadači koriste ovakve mreže u svrhe iznude – čak i protiv poslovnih rivala.

Nekoliko velikih *bot* mreža je pronadjeno i uklonjeno sa *Internet*-a. Norveški provajder *Telenor* je septembra 2004. rasformirao *bot* mrežu od oko 10 000 mašina, dok je Holandska policija oktobra 2005. uhapsila kontrolere i pronašla *bot* mrežu sa preko 1,5 miliona računara.

Tokom proteklih godina, čak je i sam DNS sistem dva puta bio napadnut DDoS metodom. Meta napada su bili jedan ili više od 13 *root* servera koji opslužuju celokupan DNS saobraćaj na *Internet*-u.

Prvi napad se dogodio 22. oktobra 2002., i trajao je oko jedan sat. Za to vreme, devet *root* servera je onеспособljeno a preostala četiri su uspela da izdrže napad. Drugi napad se dogodio 6. februara 2007. i trajao je oko pet časova. Iako nijedan od servera ovaj put nije bio oboren, dva *root* servera su prijavila „vrlo otežan rad“ dok je kod ostalih došlo do izuzetno velikog povećanja saobraćaja. *Bot* mreža koja je bila odgovorna za ovaj napad je locirana u Južnoj Koreji.



**Slika 3.6.** Kontrolni serveri i inficirani računari *bot* mreža koje prati *Shadowserver*<sup>7</sup> fondacija

Interesantno je da je samo dva dana posle drugog napada, 8. Februara 2007, časopis *Network World* objavio da je Američko Ministarstvo odbrane najavilo da bi "...u slučaju masivnog *cyber* napada na Sjedinjene Države usmerenog na narušavanje kritične informatičke infrastrukture nacije, Ministarstvo odbrane bilo spremno da pokrene *cyber* protivnapad pa čak i bombardovanje izvora tih napada."<sup>8</sup>

<sup>7</sup> <http://www.shadowserver.org>

<sup>8</sup> <http://www.networkworld.com/news/2007/020807-rsa-cyber-attacks.html>

Trenutno najveća *bot* mreža za čije se postojanje zna je *Kraken bot* mreža, otkrivena Aprila 2008. Tvrdi se da je inficirala računare u najmanje 50 kompanija sa liste *Fortune 500* i da je dostigla veličinu od preko 500.000 računara. Procenjuje se da se koristi za slanje oko 9 milijardi *spam* poruka dnevno. Takodje, smatra se da je njegov izvršni program projektovan da izbegne konvencionalni antivirusni softver, kao i IDS, IPS i *firewall* sisteme, za koje je praktično nevidljiv.

### 3.5 Fast flux

Januara 2007. otkrivena je *bot* mreža kompjutera povezana *Storm* trojancem. Do septembra 2007, procenjeno je da ta mreža kontroliše više stotina hiljada do više miliona računara kao i da predstavlja oko 8% od celokupnog malicioznog softvera prisutnog na mašinama sa *Windows* operativnim sistemom. Ono što je specifično za *Storm bot* mrežu je ujedno bio i razlog za njeno uspešno širenje. Dok se većina *bot* mreža kontroliše preko centralnog servera, koji, ako se pronadje, može biti oboren i time efektivno isključena i *bot* mreža, *Storm bot* mreža se ponaša na sličan način kao *peer-to-peer* programi, bez centralizovane kontrole. Svaka kompromitovana mašina se povezuje sa delom cele mreže – oko 30 do 35 drugih kompromitovanih mašina, koji funkcionišu kao hostovi. Dok svaki od inficiranih hostova deli liste drugih inficiranih hostova, nijedna mašina ne sadrži kompletnu listu cele mreže – svaka poseduje samo jedan deo, što procenu kompletnog obima mreže čini vrlo teškom.

Medjutim, najveća snaga *Storm bot* mreže leži u korišćenju tehnike poznate kao *fast flux*. To je tehnika koja se koristi za skrivanje sajtova za isporuku zlonamernih programa i *phishing*<sup>9</sup> sajtova iza fluktuirajuće mreže kompromitovanih hostova koji služe kao posrednici. Takodje, *fast flux* čini ovakve zlonamerne mreže izuzetno otpornim na otkrivanje i primenu protivmera.

Cilj *fast flux*-a je da se za jedan naziv domena (npr. *www.example.com*) veže veći broj (stotina pa i hiljada) IP adresa. Ove IP adrese se ubacuju i izbacuju iz optičaja izuzetno često, korišćenjem kombinacije *round robin DNS*<sup>10</sup> mehanizma i vrlo kratkih TTL<sup>11</sup> vrednosti za svaki DNS zapis resursa. Nazivi domena mogu dobijati nove IP adrese i na svakih nekoliko minuta. Korisnik koji se povezuje na isti *web* sajt kroz par minuta će se u stvari povezati sa različitom zaraženom mašinom svaki put. Takodje, napadači se brinu o tome da kompromitovani sistemi koji isporučuju njihove sadržaje imaju što veću propusnu moć i dostupnost. Koriste se i mehanizmi za raspodelu opterećenja koji proveravaju stanje svakog čvora i uklanjaju one koji nisu aktivni.

Otpornost ovakvih mreža se ostvaruje kroz posredovanje. Posredovanje ometa pokušaje da se mreža prati i uništi. Veliki broj IP adresa koje se konstantno rotiraju nisu konačno određene za zahtev za sadržajem (ili za neke druge servise). Umesto toga, kompromitovani sistemi se postavljaju samo kao posrednici koji kanališu zahteve i podatke ka i od servera u pozadini, sa kojih u stvari dolazi sadržaj. Suština je u tome da se nazivi domena za sadržaj koji se traži više ne razrešavaju na IP adresu određenog servera već fluktuiraju među mnogim posrednicima koji

<sup>9</sup> Simuliranje sigurne *web* lokacije da bi se od korisnika dobile poverljive informacije.

<sup>10</sup> Tehnika koja se inače koristi za rasterećenje *web* servera. Funkcioniše tako što na DNS upit ne odgovara uvek istom IP adresom već jednom adresom iz liste adresa (od kojih sve pretpostavljeno poseduju isti sadržaj). IP adresa sa vrha liste se šalje određen broj puta pre nego što se pomera na dno i od tog trenutka druga IP adresa iz liste postaje ona koja se vraća kao odgovor. Ovaj ciklus se neprestano ponavlja.

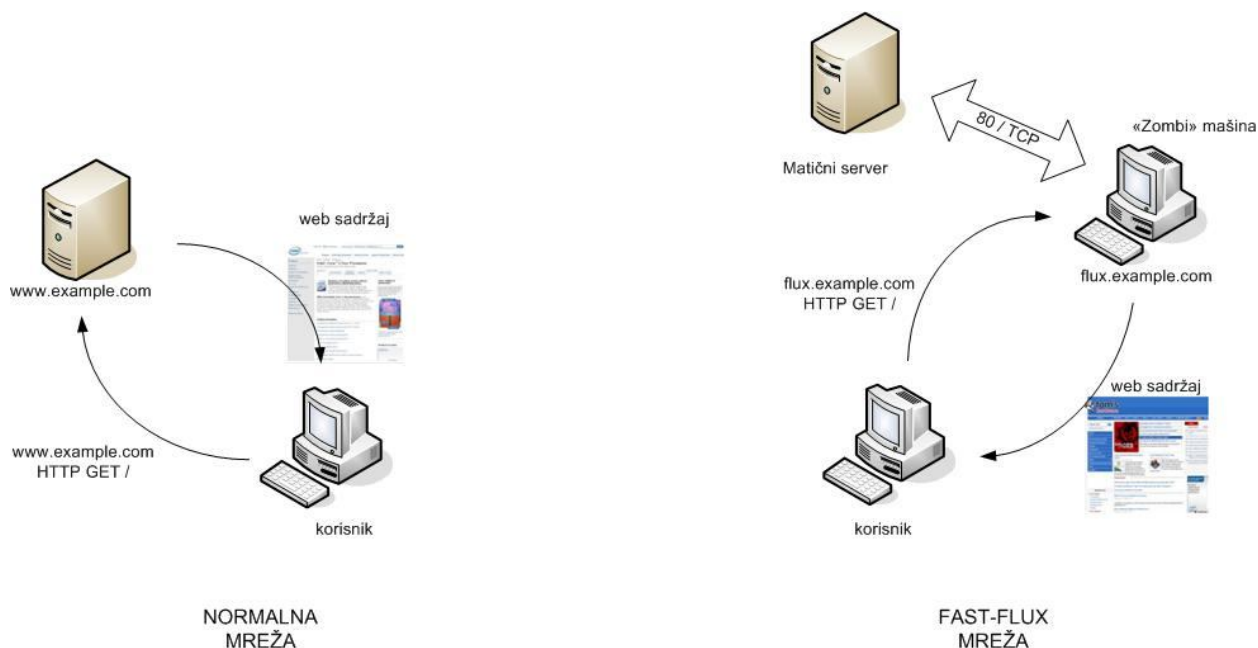
<sup>11</sup> *Time to live* (TTL) je ograničenje na vremenski period ili broj ponavljanja ili prenosa u okviru kojeg se može manipulirati paketom sa podacima pre nego što ga treba odbaciti.

prosleđuju sadržaj drugoj grupi servera u pozadini. Ova tehnika se legitimno koristi već neko vreme u svrhe održavanja visoke dostupnosti web servera i raspoređivanja opterećenja, ali u ovom slučaju predstavlja dokaz tehnološke evolucije kriminalnih kompjuterskih mreža.

Matične mašine (*motherships*) su kontrolni element *fast flux* mreža i predstavljaju ekvivalent serverima komande i kontrole koji obično postoje u konvencionalnim *bot* mrežama. Međutim, u poredjenju sa tipičnim *bot* IRC serverima, matični serveri imaju puno više uloga. Osim isporučivanja sadržaja, ovi matični čvorovi pružaju i DNS i HTTP servise sa virtuelnim hostingom koji može da opslužuje hiljade domena simultano sa jednog čvora.

Najjednostavniji oblik ove tehnike se naziva *single-flux*. Njega odlikuju sve pomenute karakteristike i mehanizmi. Sastoji se od višestrukih individualnih čvorova u okviru mreže koji vrlo često registruju i objavljuju svoje IP adrese kao deo DNS A (adresne) liste zapisa za jedan DNS naziv. Ta lista može sadržati stotine ili hiljade unosa.

U poredjenju sa normalnom komunikacijom sa web serverom, komunikacija u *single-flux* mreži se prosleđuje preko posrednika („zombi“ mašina). Dok žrtva misli da je na adresi *www.example.com*, njen internet pretraživač u stvari komunicira sa posrednikom *fast flux* mreže koji usmerava zahtev na odredišni sajt. Mreža menja DNS zapise IP adresa posrednika u periodima od čak 3-10 minuta, tako da u slučaju gašenja jednog od čvora koji obavlja posredovanje, mnogo drugih inficiranih mašina čeka spremno da zauzmu njegovo mesto. Uloga posrednika je najčešće dodeljena kompromitovanim kućnim mašinama.



**Slika 3.7.** Poredjenje komunikacije u normalnoj i *fast flux* mreži

Primer DNS zapisa za ovakve mreže je domen *divewithsharks.hk*, korišćen u već pomenute zlonamerne svrhe. U tabeli su podaci dobijeni u prvom DNS upitu za taj domen:

```
;; WHEN: Sat Feb 3 20:08:08 2007

divewithsharks.hk. 1800 IN A 70.68.187.xxx [xxx.vf.shawcable.net]
divewithsharks.hk. 1800 IN A 76.209.81.xxx [SBIS-AS - AT&T Internet Services]
divewithsharks.hk. 1800 IN A 85.207.74.xxx [adsl-usti1xxx-74-207-85.bluetone.cz]
divewithsharks.hk. 1800 IN A 90.144.43.xxx [d90-144-43-xxx.cust.tele2.fr]
divewithsharks.hk. 1800 IN A 142.165.41.xxx [142-165-41-xxx.msju.hsdb.sasknet.sk.ca]

divewithsharks.hk. 1800 IN NS ns1.world-wr.com.
divewithsharks.hk. 1800 IN NS ns2.world-wr.com.

ns1.world-wr.com. 87169 IN A 66.232.119.xxx [HVC-AS - HIVELOCITY VENTURES CORP]
ns2.world-wr.com. 87177 IN A 209.88.199.xxx [vpdn-dsl209-88-199-xxx.alami.net]
```

Oko 30 minuta kasnije, dolazi do promene u zapisima:

```
;; WHEN: Sat Feb 3 20:40:04 2007 (~30 minuta/1800 sekundi kasnije)

divewithsharks.hk. 1800 IN A 24.85.102.xxx [xxx.vs.shawcable.net] NOVA
divewithsharks.hk. 1800 IN A 69.47.177.xxx [d47-69-xxx-177.try.wideopenwest.com] NOVA
divewithsharks.hk. 1800 IN A 70.68.187.xxx [xxx.vf.shawcable.net]
divewithsharks.hk. 1800 IN A 90.144.43.xxx [d90-144-43-xxx.cust.tele2.fr]
divewithsharks.hk. 1800 IN A 142.165.41.xxx [142-165-41-xxx.msju.hsdb.sasknet.sk.ca]

divewithsharks.hk. 1800 IN NS ns1.world-wr.com.
divewithsharks.hk. 1800 IN NS ns2.world-wr.com.

ns1.world-wr.com. 85248 IN A 66.232.119.xxx [HVC-AS - HIVELOCITY VENTURES CORP]
ns2.world-wr.com. 82991 IN A 209.88.199.xxx [vpdn-dsl209-88-199-xxx.alami.net]
```

Dve označene IP adrese su promenjene. Ponovo, ove adrese pripadaju *dial-up* ili *broadband* kućnim korisnicima. Posle sledećih 30 minuta:

```
;; WHEN: Sat Feb 3 21:10:07 2007 (~30 minuta/1800 sekundi kasnije)

divewithsharks.hk. 1238 IN A 68.150.25.xxx [xxx.ed.shawcable.net] NOVA
divewithsharks.hk. 1238 IN A 76.209.81.xxx [SBIS-AS - AT&T Internet Services] Već korišćena!
divewithsharks.hk. 1238 IN A 172.189.83.xxx [xxx.ipt.aol.com] NOVA
divewithsharks.hk. 1238 IN A 200.115.195.xxx [pcxxx.telecentro.com.ar] NOVA
divewithsharks.hk. 1238 IN A 213.85.179.xxx [CNT Autonomous System] NOVA

divewithsharks.hk. 1238 IN NS ns1.world-wr.com.
divewithsharks.hk. 1238 IN NS ns2.world-wr.com.

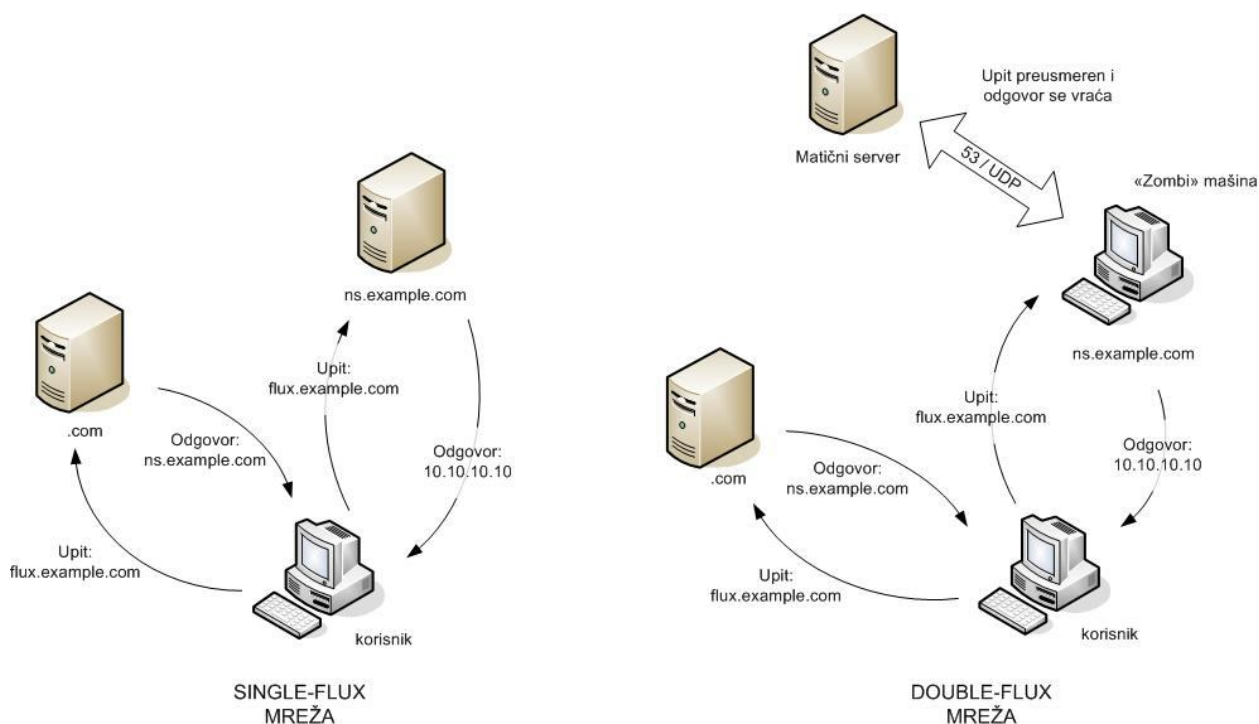
ns1.world-wr.com. 83446 IN A 66.232.119.xxx [HVC-AS - HIVELOCITY VENTURES CORP]
ns2.world-wr.com. 81189 IN A 209.88.199.xxx [vpdn-dsl209-88-199-xxx.alami.net]
```

Ovde se mogu primetiti četiri nove IP adrese i jedna koja je već postojala u prvom upitu. Kao što se iz primera vidi, A zapisi za domen se konstantno menjaju. Svaki od ovih sistema predstavlja kompromitovanu mašinu koja radi kao posrednik, koji eventualno vodi do zlonamernog sadržaja.

Sofisticiraniji tip *fast flux* tehnike je *double-flux*. Njega karakterišu višestruki čvorovi unutar mreže koji vrlo često registruju i odjavljuju svoje IP adrese kao deo DNS NS<sup>12</sup> liste zapisa za DNS zonu. Ovo obezbeđuje dodatni nivo redundantnosti i otpornosti unutar mreže.

Komunikacija je donekle slična onoj kod *single-flux* mreža. U *single-flux* mrežama, klijent šalje upit *root* serveru naziva za adresom servera autoritativnom za *.com* domen. U sledećem koraku, klijent šalje upit *.com* serveru naziva za domen *example.com* i dobija odgovor da treba da se obrati serveru naziva *ns.example.com*. Klijent sada šalje upit autoritativnom DNS serveru *ns.example.com* za adresu *flux.example.com*. Server odgovara IP adresom sa kojom klijent pokušava da ostvari komunikaciju. U normalnim okolnostima ova IP adresa ostaje konstantna duže vreme, dok se kod *single-flux* mreža ona menja iz minuta u minut.

Kod *double-flux* mreža, klijent prvo vrši upit za adresom *flux.example.com*. Ponovo, prvi korak je upit ka *root* serveru naziva. Zatim, klijent šalje upit serveru naziva odgovornom za *.com* domen i traži autoritativni server naziva za domen *example.com*. U trećem koraku, klijent šalje upit autoritativnom serveru naziva *ns.example.com* za adresu *flux.example.com*. Međutim, ovaj autoritativni server naziva je u stvari i sam deo *double-flux* mehanizma, i njegova IP adresa se često menja. Kada dobije DNS upit za *flux.example.com* od klijenta, server prosledjuje upite matičnom serveru radi dobijanja potrebnih informacija. Klijent tada može pokušati da uspostavi direktnu komunikaciju sa traženim sistemom (dok će i ovaj sistem i sam biti jedan od posredničkih čvorova koji se dinamički menjaju).



Slika 3.8. Poredjenje *single-flux* i *double-flux* mreže

<sup>12</sup> Name Server (NS) zapis mapira naziv domena ka listi DNS servera koji su autoritativni za taj domen.

Primer za ovakvu vrstu mreža može biti *phishing* napad usmeren protiv popularnog sajta *MySpace*. Napadač je kreirao lažni sajt pod imenom *login.mylspacee.com*. Ovaj sajt vizuelno izgleda kao stvarni *MySpace* sajt ali umesto toga prikuplja podatke o *MySpace* korisnicima od svakog ko bude prevaren da se uloguje na lažni sajt. Ovaj put i NS i DNS A zapisi se konstantno menjaju:

```
;; WHEN: Wed Apr 4 18:47:50 2007

login.mylspacee.com. 177 IN A 66.229.133.xxx [c-66-229-133-xxx.hsd1.fl.comcast.net]
login.mylspacee.com. 177 IN A 67.10.117.xxx [cpe-67-10-117-xxx.gt.res.rr.com]
login.mylspacee.com. 177 IN A 70.244.2.xxx [adsl-70-244-2-xxx.dsl.hrlntx.swbell.net]
login.mylspacee.com. 177 IN A 74.67.113.xxx [cpe-74-67-113-xxx.stny.res.rr.com]
login.mylspacee.com. 177 IN A 74.137.49.xxx [74-137-49-xxx.dhcp.insightbb.com] ]

myspacee.com. 108877 IN NS ns3.myheroisyourslove.hk.
myspacee.com. 108877 IN NS ns4.myheroisyourslove.hk.
myspacee.com. 108877 IN NS ns5.myheroisyourslove.hk.
myspacee.com. 108877 IN NS ns1.myheroisyourslove.hk.
myspacee.com. 108877 IN NS ns2.myheroisyourslove.hk.

ns1.myheroisyourslove.hk. 854 IN A 70.227.218.xxx [ppp-70-227-218-xxx.dsl.sfldmi.ameritech.net]
ns2.myheroisyourslove.hk. 854 IN A 70.136.16.xxx [adsl-70-136-16-xxx.dsl.bumttx.sbcglobal.net]
ns3.myheroisyourslove.hk. 854 IN A 68.59.76.xxx [c-68-59-76-xxx.hsd1.al.comcast.net]
ns4.myheroisyourslove.hk. 854 IN A 70.126.19.xxx [xxx-19.126-70.tampabay.res.rr.com]
ns5.myheroisyourslove.hk. 854 IN A 70.121.157.xxx [xxx.157.121.70.cfl.res.rr.com]
```

Oko 4 minuta kasnije, promenjeni su samo A zapisi. NS zapisi su ostali isti:

```
;; WHEN: Wed Apr 4 18:51:56 2007 (~4 minuta/186 sekundi kasnije)

login.mylspacee.com. 161 IN A 74.131.218.xxx [74-131-218-xxx.dhcp.insightbb.com] NOVA
login.mylspacee.com. 161 IN A 24.174.195.xxx [cpe-24-174-195-xxx.elp.res.rr.com] NOVA
login.mylspacee.com. 161 IN A 65.65.182.xxx [adsl-65-65-182-xxx.dsl.hstntx.swbell.net] NOVA
login.mylspacee.com. 161 IN A 69.215.174.xxx [ppp-69-215-174-xxx.dsl.ipltin.ameritech.net] NOVA
login.mylspacee.com. 161 IN A 71.135.180.xxx [adsl-71-135-180-xxx.dsl.pltn13.pacbell.net] NOVA

myspacee.com. 108642 IN NS ns3.myheroisyourslove.hk.
myspacee.com. 108642 IN NS ns4.myheroisyourslove.hk.
myspacee.com. 108642 IN NS ns5.myheroisyourslove.hk.
myspacee.com. 108642 IN NS ns1.myheroisyourslove.hk.
myspacee.com. 108642 IN NS ns2.myheroisyourslove.hk.

ns1.myheroisyourslove.hk. 608 IN A 70.227.218.xxx [ppp-70-227-218-xxx.dsl.sfldmi.ameritech.net]
ns2.myheroisyourslove.hk. 608 IN A 70.136.16.xxx [adsl-70-136-16-xxx.dsl.bumttx.sbcglobal.net]
ns3.myheroisyourslove.hk. 608 IN A 68.59.76.xxx [c-68-59-76-xxx.hsd1.al.comcast.net]
ns4.myheroisyourslove.hk. 608 IN A 70.126.19.xxx [xxx-19.126-70.tampabay.res.rr.com]
ns5.myheroisyourslove.hk. 608 IN A 70.121.157.xxx [xxx.157.121.70.cfl.res.rr.com]
```

Oko sat i po kasnije, NS zapisi za ovaj domen su pomereni i pojavljuje se pet novih NS zapisa. Slično prethodnom primeru, A i NS zapisi pripadaju *dial-up* i *broadband* provajderima, što je dobar znak da se radi o kompromitovanim mašinama koje bivaju zloupotrebljene:

```
;; WHEN: Wed Apr 4 21:13:14 2007 (~90 minuta /4878 sekundi kasnije)

ns1.myheroisyourslove.hk. 3596 IN A 75.67.15.xxx [c-75-67-15-xxx.hsd1.ma.comcast.net] NOVA
ns2.myheroisyourslove.hk. 3596 IN A 75.22.239.xxx [adsl-75-22-239-xxx.dsl.chcgil.sbcglobal.net] N
ns3.myheroisyourslove.hk. 3596 IN A 75.33.248.xxx [adsl-75-33-248-xxx.dsl.chcgil.sbcglobal.net] N
ns4.myheroisyourslove.hk. 180 IN A 69.238.210.xxx [ppp-69-238-210-xxx.dsl.irvnca.pacbell.net] NOV
ns5.myheroisyourslove.hk. 3596 IN A 70.64.222.xxx [xxx.mj.shawcable.net] NOVA
```

Mreže koje koriste *fast flux* predstavljaju evolutivni korak za kriminal na Internetu. Ovakve mreže stvaraju robustne, obskurne infrastrukture koje čine zadatak uklanjanja aktivnih prevara i identifikovanja kriminalaca koji njima upravljaju naročito teškim kako za sistem administratore tako i za organe pravosuđa. Robustnost, mogućnosti prikrivanja, skalabilnost kao i sve veća pojava *bot* mreža koje koriste *fast flux* tehnike donose sve veću dobit kriminalcima koji njima upravljaju.

Kao i za legitimne poslove, Internet predstavlja veliko plodno ekonomsko tle za kriminal, što znači da će tehnike kao što je *fast flux* nastaviti da se razvijaju. Nažalost, često su ovakve pretnje korak ispred profesionalaca koji se bave pitanjima bezbednosti na mreži.

### 3.5.1 Storm bot mreža

*Storm bot* mreža je korišćena u mnoštvu kriminalnih aktivnosti. Njeni kontroleri, kao i autori *Storm* crva, još uvek nisu identifikovani. *Storm bot* mreža pokazuje odbrambeno ponašanje koje nagoveštava da njeni kontroleri aktivno brane mrežu od pokušaja da se ona prati i onespobi. Mreža je napadala online segmente nekih kompanija koje se bave mrežnom bezbednošću kao i istraživača koji su pokušali da saznaju više o njoj. Većina eksperata za bezbednost se slaže da će ova bot mreža predstavljati veliki bezbednosni rizik i u budućnosti a Američki FBI smatra ovu mrežu značajnim izvorom bankarskih prevara, krađa identiteta i drugih oblika sajber-kriminala.

Pri pokretanju *Storm* crva, on pokušava da se poveže sa drugim inficiranim hostovima putem *peer-to-peer* umrežavanja. Kroz ovaj kanal, crv saznaje URL koji pokazuje na izvršni fajl druge etape, u kojoj se na zaraženi računar preuzimaju naredne etape.

Ove etape obično nose ime od *game0.exe* do *game5.exe* i svaka komponenta ima specifičnu funkciju:

*game0.exe* – Backdoor/downloader

*game1.exe* – SMTP prosledjivač

*game2.exe* – Alat za krađu email adresa

*game3.exe* – Alat za širenje email virusa

*game4.exe* – DDoS alat

*game5.exe* – Nova, ažurirana kopija *Storm* crva

Glavna komponenta se pokreće iz kernel *rootkit* drajvera (%windir%\system32\wincom.sys), koji ubacuje svoj kod u proces *services.exe*. Ovo je deo koji je odgovoran za povezivanje na P2P mrežu.

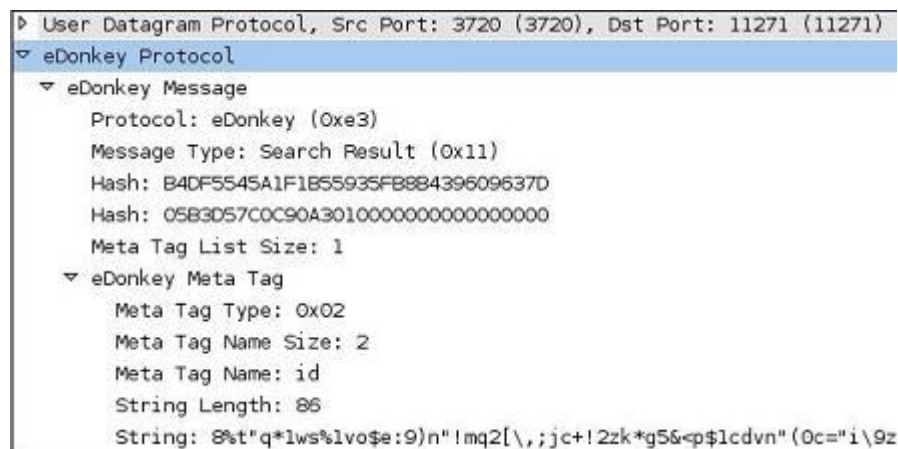
Protokol koji se koristi je u stvari *eDonkey/Overnet* protokol, koji je modifikovan od strane autora virusa da bude način za distribuciju URL adrese druge faze, izbegavajući gašenje koje bi usledilo da je URL trajno upisan u telu virusa ili da se preuzima sa drugog sajta.

P2P komponenta sadrži trajno upisanu listu preko 100 čvorova u telu trojanca, koje snima u `%windir%\system32\wincom.ini`.

```
D943283AB63746B8E62436682728DDD4=5511238154BD00
D6E46BF02E64D940E37EECC982584A8=573349B6124A00
AA71F6CB9B9BB53D9FA47B74B189E67E=8002DE60541D00
91692CA8A8B7F9DA5E68E749CD8E9BF6=968C8C30276A00
90574FE5893DC69889C2E041CE549CF7=55193625196A00
87E19465E6C768A9AF641261EE3F264F=530EDD0A4AF800
83A420370958C05DD460005C27AF0883=DD82082C420200
5C4C83F5CA7CC5FC96B67BF2AFC0A0F6=434E515D185D00
5194784563D5B072109A7EBE6C2DDD1E=578B1AD02FC300
4C09AD9D350ABAFD51A5C76A5DC10C54=58BF246B518C00
...
```

Deo ispred znaka jednakosti predstavlja sažetak (*hash*) čvora, a deo posle njega je IP adresa i port. Na primer, `5511238154BD00 = 0x55.0x11.0x23.0x81:0x54BD` ili `85.17.35.129:21693`. Ovi čvorovi se kontaktiraju i trojanac proverava da li oni imaju određeni sažetak koji se traži. Ako sažetak nije nadjen, ovi čvorovi usmeravaju inficiranog klijenta na druge čvorove koji mogu da sadrže traženi sažetak, sve dok se on ne nadje.

U uobičajenoj *eDonkey/Overnet* razmeni, vrednost sažetka predstavlja MD4 zbir datoteke na čvoru. U P2P kodu *Storm* crva, sažetak se u stvari ne odnosi na datoteku, već se generiše uz pomoć algoritma koji kao ulaz uzima trenutno sistemsko vreme i slučajni broj izmedju 0 i 31, dajući na izlazu jedan od 32 moguća sažetka za bilo koji dan.



**Slika 3.9.** *eDonkey/Overnet* protokol koji koristi *Storm* crv

Kada neki od čvorova odgovori rezultatom pretrage koji sadrži traženi sažetak, on vraća traženi sažetak, kao i sažetak „rezultata“, u paketu koji se šalje kao odgovor (na slici to je `05B3D57C0C90A3010000000000000000`). Ovaj sažetak služi P2P kodu *Storm* crva kao ključ za dešifrovanje, zajedno sa drugim ključem za dešifrovanje koji je trajno upisan u telu samog trojanca. Takodje, u paketu koji se šalje kao odgovor postoji meta-tag sa nazivom *id*. Telo ovog taga sadrži šifrovani string sa URL adresom izvršne datoteke druge etape. Nikada se ne prenose fajlovi izmedju hostova – meta tag i sažetak rezultata pretrage su jedine stvari koje su trojancu potrebne od čvorova da bi pronašao sajt za preuzimanje.

### 3.5.2 DDoS Funkcionalnost

DDoS napad izvodi izvršna datoteka *game4.exe*. Ona dobija IP adresu mete kao i tip napada preuzimajući konfiguracionu datoteku sa trajno upisane *web* adrese u telu trojanca. Napadi mogu predstavljati *TCP syn flood*<sup>13</sup> na portu 80 ili *ICMP ping flood*<sup>14</sup>, ili oboje. Konfiguraciona datoteka obezbeđuje samo IP adresu; ovaj alat nema mogućnosti da samostalno razrešava DNS nazive u adrese.

Pored *anti-spam* sajtova koji su napadani, u konfiguracionoj datoteci su vidjani i IP adrese sajtova koji su povezani sa *Wareзов* virusom – još jednim *spam* sistemom, koju verovatno kontroliše konkurentska *spam* grupa. Izgleda da je ova spammerska grupa spremna da napadne bilo koga ko ometa njihov poslovni model, bilo da je u pitanju *anti-spam* organizacija ili druga *spam* grupa, pa u nekim slučajevima i neka treća strana. Na primer, jedna IP adresa koja je napadana je bila *capitalcollect.com*, servis za transfer novca. Neke od IP adresa koje su bile meta DDoS komponente *Storm* crva januara 2007, obuhvatale su

| IP adresa mete | Naziv domena                                       |
|----------------|----------------------------------------------------|
| 67.15.52.145   | stockpatrol.com                                    |
| 63.251.19.36   | spamnation.info                                    |
| 216.118.117.38 | esunhuitionkdefunhsadwa.com ( <i>Wareзов</i> )     |
| 208.66.194.155 | krovalidajop.com, traferreg.com ( <i>Wareзов</i> ) |
| 66.246.246.69  | shionkertunhedanse.com ( <i>Wareзов</i> )          |
| 69.72.215.236  | capitalcollect.com                                 |
| 208.66.72.202  | adesuikintandefunhandesun.com ( <i>Wareзов</i> )   |
| 66.246.252.206 | huirefunkionmdesa.com ( <i>Wareзов</i> )           |

**Tabela 3.1.** Delimična lista IP adresa koje je napadao *Storm* crv

Interesantno je da je januara 2007 napadan još jedan domen – *spamhaus.org*, saobraćajem koji je bio jako sličan paketima koji su korišćeni u prethodnim napadima. Međutim, brzo je postalo jasno da taj sajt nije bio prava meta – operateri *Wareзов* sistema su, u pokušaju da odbiju DDoS napad, promenili A zapise u DNS-u za neke od svojih domena na taj način da pokazuju na *spamhaus.org* IP adresu. Kada je DDoS datoteka *Storm* crva preuzela novu verziju sa promenjenom IP adresom, napad na *spamhaus.org* je počeo.

Kako je u ovom trenutku praktično nemoguće utvrditi odgovorne za ove napade, i da samim tim oni u ovom trenutku ne snose nikakve posledice, izgleda da je sve više spamera voljno i sposobno da napadne bilo koga ko se pojavi kao pretnja njihovom profitu.

### 3.5.3 Šifrovanje i prodaja

Krajem 2007, otkriveno je da bi delovi *Storm bot* mreže kao i njenih varijanti mogli biti ponudjeni na prodaju ili iznajmljivanje. Ovo je realizovano korišćenjem jedinstvenih bezbednosnih ključeva u šifrovanju internet saobraćaja *bot* mreže. Jedinstveni ključevi omogućavaju svakom segmentu ili delu *Storm bot* mreže da komunicira sa segmentom koji sadrži isti ključ.

<sup>13</sup> DoS napad u kome napadač šalje veliki niz SYN zahteva napadanom sistemu.

<sup>14</sup> DoS napad u kome napadač obasipa žrtvu velikim brojem ICMP *Echo* paketima (*ping*-ovima)

Početkom 2008, primećeno je da je ova mreža počela da bude upotrebljavana u *phishing* napadima protiv velikih finansijskih institucija kao što su *Barclays*, *Halifax Bank*, *Royal Bank of Scotland* itd.

### 3.5.4 Borba protiv fast-flux mreža

Do skoro je bilo lako locirati i ukloniti lokacije gde je čuvan zlonamerni softver kao i maliciozne web sajtove. Bili su ili registrovani u DNS-u ili koristili svoje IP adrese. Jedan poziv ili e-mail odeljenju za zloupotrebe i internet provajder je bio jedina potrebna mera. Sa pojavom bot mreža, sve se to promenilo.

Tehnologija bot mreža je promenila shvatanje hakerisanja. Umesto kontrole nad malim brojem mašina i korišćenjem tih mašina za pokretanje napada, zlonamerni pojedinci sada mogu da kontrolišu stotine, hiljade pa i više mašina koje onda mogu koristiti za još veći broj napada. Identifikovanje svih dronova u bot mreži je postalo jako teško zbog same veličine mreže. Čak i posle identifikovanja mašina, one bi se često prosto ponovo inficirale. Zbog toga je pažnja usmerena ka strukturi komande i kontrole bot mreže. Ovo je za rezultat imalo pojavu *fast-flux* mreža koje omogućavaju korišćenje velikog broja zaraženih mašina i DNS-a za brzo usmeravanje i preusmeravanje žrtava ka zlonamernim web sajtovima i mehanizmima komande i kontrole.

Da bi se pretnja *fast-flux* mreža što više ublažila, predložen je niz promena u DNS standardu. Predlog promena je objavljen Maja 2008. kao dokument *Double Flux Defense in DNS*<sup>15</sup> i trenutno se vodi kao nacrt. Predložene promene obuhvataju različite nivoe:

- Promene kod registrara

Registrarovi bi trebalo da ograniče dozvoljeni period u kome se mogu vršiti promene na autoritativnim DNS serverima za domene pod njihovom kontrolom na jedan set promena u okviru 72 časa. Trebalo bi dozvoliti i vraćanje na stara podešavanja u slučaju greške, koje bi vratilo podešavanja na stanje pre promene i restartovalo brojač na 72 časa. Ovo bi sprečilo zlonamerne pojedince da konstantno menjanju DNS zapise da bi izbegli gašenje.

- Promene u autoritativnim DNS servisima

Za vreme pokretanja, DNS servisi bi trebalo da provere TTL kako za NS zapise tako i za A zapise vezane za njih. Ako je TTL vreme postavljeno na manje od 86400 (24 časa) trebalo bi da bude automatski promenjeno na 259200 (72 časa) i da se taj događaj ubeleži u sistemski log. Vrednosti između 24-72 časa bi bile moguće ali bi sve vrednosti ispod 24 časa automatski bile promenjene na 72 časa.

- Promene u DNS servisima za razrešavanje

DNS serveri koji nisu autoritativni ali koji vrše upite za lokalne klijente bi trebalo da proveravaju TTL za NS zapis, i ako je moguće, A zapis odgovarajućeg servera naziva.

<sup>15</sup> <http://tools.ietf.org/html/draft-bambenek-doubleflux-01>

Ako se kao odgovor na bilo koji upit dobije TTL vrednost manja od 12 časova, trebalo bi da bude odbačen i vraćena poruka o grešci bez obaveštavanja klijenta koji je postavio upit.

- Promene na DNS klijentima

DNS klijenti bi trebalo da proveravaju vraćene TTL vrednosti NS zapisa (i odgovarajuće A zapise za te NS zapise) za sve upite na servera naziva gde se kao odgovor dobije vrednost manja od 12 časova. Ako se primi odgovor sa malim TTL vremenom, trebalo bi da bude odbačen, bez davanja IP adrese aplikaciji koja je uputila zahtev.

Promene koje se predlažu ovim merama menjaju DNS protokol radi poboljšanja bezbednosti u postojećim sistemima. One ne sprečavaju zloupotrebu, ali mogu da uspore širenje malicioznih DNS promena i tako dozvole preduzimanje odgovarajućih korektivnih mera. Ovo teoretski poboljšava bezbednost DNS servisa.

## 4. Budućnost Internet-a i DNS-a

---

### 4.1 ICANN i administracija DNS-a

Iako je opšte poznato da je *Internet* decentralizovan i nehijerarhijski organizovan, u njegovoj osnovi je i dalje centralizovana hijerarhija, što se najbolje vidi posmatranjem DNS-a. Potreba da se obezbedi jedinstvenost, tj. da se spreči korišćenje duplih naziva domena, stvorila je potrebu za nekom vrstom tela koje bi pratilo ili dodeljivalo imena. Međutim, kontrola nad DNS-om daje značajnu moć nad *Internet*-om. Ko god kontroliše DNS, odlučuje koji novi TLD nazivi mogu da se uvedu (npr. novi sufixi kao što je *.xxx* ili *.shop*) i kako će imena i IP adrese biti dodeljene *web* sajtovima i drugim *Internet* resursima.

Kada je *Internet* još bio u začetku, DNS je održavala grupa volontera, zajedno sa Američkom Nacionalnom Naučnom Fondacijom (NSF) i civilnim i vojnim preduzimačima. Eksplozivni rast *Internet*-a je otežao funkcionisanje u to vreme *ad hoc* sistema za upravljanje DNS-om, i ono što su u početku bila uglavnom tehnička pitanja, postala su politički, pravni i ekonomski problemi koji su počeli da privlače zvaničnu pažnju. Naročito, od kada su atraktivni nazivi *.com* domena postali retki, sporovi oko ovakvih imena su postali uobičajeni i počeo je da raste pritisak da se otvore novi domeni najvišeg nivoa, kao što je *.web*. Iako tehnički trivijalno za implementaciju, predlog je dočekan sa neodobravanjem od strane nosioca intelektualnih svojina koji su se već suočavali sa sve većim problemima sa licima koja su registrovala nazive domena koja su odgovarala zaštitnim znacima i držala ih radi profita. Za to vreme, vlade drugih zemalja, naročito u Evropskoj Uniji, su počele da izražavaju razumljivu zabrinutost zbog kontrole koju Sjedinjene Države imaju nad kritičnim elementom globalnog komunikacionog i komercijalnog resursa, od kojeg će njihove ekonomije i društva sve više zavisiti.

Juna 1998, Američko Ministarstvo trgovine je kao odgovor na sve veću zabrinutost vezanu za DNS, donelo Izjavu o politici privatizacije adresnog prostora na *Internetu*, poznatu kao *DNS White Paper*<sup>16</sup>. Ovaj dokument je pozvao na formiranje privatne neprofitne korporacije koja bi preuzela DNS i izvršila različite reforme. Nedugo posle toga, međunarodna grupa je posle zatvorenog sastanka, objedinjena u ICANN, kao privatnu neprofitnu korporaciju sa sedištem u Kaliforniji. Nedugo zatim, Američko Ministarstvo trgovine je prenelo na ICANN većinu svojih ovlašćenja vezanih za upravljanje DNS-om.

U prve dve godine postojanja, ICANN je uveo nekoliko promena sa potencijalno dugoročnim efektima.

Uvedena je obavezna arbitraža žalbi na korišćenje zaštitnih znakova. ICANN-ova Jednoobrazna politika razrešavanja sporova<sup>17</sup> (*Uniform Dispute Resolution Policy* – UDRP) zahteva od svake strane registrovane pod *.com*, *.org* i *.net* domenima da prihvati arbitražu pred

---

<sup>16</sup> [http://www.ntia.doc.gov/ntiahome/domainname/6\\_5\\_98dns.htm](http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm)

<sup>17</sup> <http://www.icann.org/udrp/udrp.htm>

ICANN-ovom komisijom ako bilo koji vlasnik bilo gde u svetu izrazi sumnju da je registrovani naziv sličan njihovom zaštitnom znaku. Sam UDRP dokument je veoma kontroverzan – vlasnici zaštitnih znakova se žale da nije dovoljno strog; grupe za građanska prava tvrde da takav sistem krši osnovne norme fer procesa i da se komisija ne ponaša nepristrasno.

Takodje, suprotno ranijim obećanjima da će polovina Saveta Direktora biti izabrana iz nezavisnog članstva, ICANN je objavio: da neće postojati članstvo, da će samo 5 od 18 umesto 9 od 18 njegovih direktora biti slobodno izabrano, da će četiri od inicijalno izabranih direktora ostati na funkciji i da će ICANN sprovesti analizu da bi odredio da li bi uopšte trebalo da postoje nezavisno birani direktori.

Ono što predstavlja najveći problem, i što u stvari predstavlja izvor zabrinutosti, je što, istorijski gledano, nedostatak odgovornosti uvek dovodi do samovolje. Pored toga što nema odgovornost prema vladi, ICANN nema ni mehanizme kontrole odgovornosti koji obično postoje u korporacijama ili neprofitnim organizacijama. Takodje, ICANN nema problema sa finansijama, budući da su *Internet* registri prihvatili ICANN-ov autoritet i uplatu povremenih priloga u zamenu za mogućnost da prodaju registracije u *.com*, *.net* i *.org* domenima.

Rezultat ovakve istorije je telo sa minimalnom odgovornošću. Ovaj problem će samo postati veći ako Američko Ministarstvo trgovine prenese ICANN-u punu kontrolu nad DNS-om, jer najvažniji deo bilo čije „kontrole“ nad *root*-om u stvari predstavlja objavljivanje podataka na koje se različite strane, od kojih su mnoge nevladine, oslanjaju.

Događaj sa početka 2007. godine je samo povećao sumnje koju ova tema izaziva. Marta 2007, na godišnjem sastanku ICANN-a u Lisabonu, predsednik Kanadske Agencije za *Internet* registraciju, kao predstavnik registara nacionalnih domena najvišeg nivoa, je saopštio da Američki *Department of Homeland Security* želi da ključ za potpisivanje DNS *root* zone (ključ za potpisivanje ključeva zona, trenutno u rukama *VeriSign*-a) bude pod kontrolom Vlade SAD<sup>18</sup>. DHS trenutno sponzorise kampanju za podršku implementacije DNSsec-a.

Uključivanje DHS-a u razvoj DNSsec-a nije iznenađujuće u smislu da je učešće vlade neophodno pri istraživanju i razvoju novih tehnologija (rani *Internet* je dobar primer). Ali, ponovo istorijski gledano, vlade su često pokušavale da utiču na tehničke standarde u cilju zaštite domaće industrije, povećanja sopstvene moći ili sticanja ekonomske dobiti. Ono što je interesantno sa stanovišta uvođenja DNSsec-a je interesovanje koju DHS ima za bezbednost ostalih važnih *Internet* standarda (kao što je inicijativa za bezbednost protokola za rutiranje, SPRI<sup>19</sup>) i široko verovanje da su aktivnosti ključnih organizacija koje se bave infrastrukturom *Internet*-a vođene interesima privatnog sektora. Uz činjenicu da je infrastruktura *Internet*-a po svojoj prirodi međunarodna i da se globalna ekonomija oslanja na nju, zabrinutost koju ova pitanja izazivaju je razumljiva.

*VeriSign*-ov ekspert za DNSsec, dr *Phillip Hallam-Baker*, objavio je na IETF mailing listi<sup>20</sup> tekst o implikacijama potpisivanja *root*-a korišćenjem DNSsec-a. Takodje, pozvao je na deljenje ovlašćenja za potpisivanje:

“...Treba uzeti u obzir da je ovo infrastruktura koja bi trebalo da bude robusna tokom nekoliko dekada, ako ne i vekova. Takodje, treba razmotriti i verovatnoću da ko god kontroliše

<sup>18</sup> <http://www.heise.de/english/newsticker/news/87655>

<sup>19</sup> <http://www.cyber.st.dhs.gov/spri.html>

<sup>20</sup> <http://www1.ietf.org/mail-archive/web/ietf/current/thrd4.html>

*root*, može preduzeti neki postupak koji neka druga strana, u tako dugom vremenskom periodu, može smatrati odmetanjem.”

“Na primer, mala ali uticajna grupa glasača na jugozapadnom poluostrvu države A smatra sebe političkim prognanicima iz države B, ostrva u blizini poluostrva. Država A je u jedinstvenoj poziciji da utiče na *root* i pomenuti glasači lobiraju za izuzimanje države B. Ako bi do ovoga došlo danas, rezultat bi bio privremeno cepanje *root*-a praćeno brzim pojavljivanjem alternativne *root* strukture koja nije bila pod zloupotrebom države A. Strane imaju vlast ali nemaju moć. Ako bi *root* bio potpisan od strane jedinstvenog tela, to telo bi imalo apsolutnu moć. Odmetanju se ne bi moglo suprotstaviti cepanjem *root*-a. Danas se prostor za odmetanje drži u ravnoteži nedostatkom bezbednosti. *Root* se, konačno, definiše lokacijom na koju određeni provajder usmerava UDP pakete sa IP adresom *root* servera. Posle potpisivanja, *root* bi bio definisan poznavanjem privatnog ključa koji bi odgovarao široko distribuiranim i ugrađenim javnim ključem.”

“Uzmite u obzir činjenicu da Evropa trenutno planira kopiranje GPS satelitskog sistema po ceni od nekoliko milijardi dolara uprkos činjenici da je jedini razlog za to sprečavanje sličnog odmetanja od strane Sjedinjenih Država. Ideja da kontrola DNS *root*-a ne bi bila izložena i značajnijim geo-političkim pritiscima je naivna. 1955. bi postavljanje ovog sistema bilo obavljeno bez privlačenja nepotrebne pažnje, što nije slučaj danas.”

## 4.2 Alternativni DNS

Uz postojećih 13 DNS root servera koji rade u dogovoru sa ICANN-om, nekoliko organizacija upravlja alternativnim DNS root serverima. Svaka od njih poseduje sopstvenu grupu root servera naziva i sopstveni skup *top level* domena.

Alternativni root serveri najčešće obuhvataju adresiranje za sve TLD servere koje je odredio ICANN (generički *.com*, *.net*, *.org*... kao i državni *.rs*, *.uk* itd.), kao i za TLD servere za druge domene najvišeg nivoa (kao što su *.new*, *.web*, *.tech*...) koje ICANN nije definisao, već ih održavaju nezavisne organizacije. Neke, ali ne sve alternativne root servere održavaju organizacije koje istovremeno upravljaju i ovim alternativnim TLD domenima.

Razlozi za pokretanje alternativnog adresiranja mogu biti različiti, ali se uopšteno mogu podeliti na sisteme: Pokrenute iz idealističkih ili ideoloških razloga, kao komercijalni projekti i kao interni projekti organizacija za sopstvene potrebe.

Trenutno samo mali deo provajdera koristi usluge alternativnih root servera, dok se većina drži servera koje je naveo ICANN. *Internet Architecture Board*<sup>21</sup> se u dokumentu RFC 2826 snažno protivi postavljanju i korišćenju alternativnih root servera naziva.

Najozbiljniji projekat alternativnog sistema adresiranja na Internetu predstavlja *Open Root Server Network* (ORSN)<sup>22</sup>, koji funkcioniše od 2002. Njegova root zona se obično održava u sinhronizaciji sa mrežom koju koordinira ICANN. Mreže su stoga kompatibilne, iako ORSN funkcioniše potpuno nezavisno od ICANN-a. Njegovi serveri su uglavnom smešteni u Evropi.

<sup>21</sup> Komitet zadužen za nadgledanje tehničkog razvoja Interneta. Nadgleda više radnih grupa, uključujući IETF

<sup>22</sup> <http://www.orsn.org>

Osnivači ORSN mreže su kao glavni razlog pokretanja naveli zabrinutost zbog uticaja koji vlada SAD ima na ICANN. Njihov cilj je da ograniče kontrolu nad Internet-om koju daju root serveri, ali obezbeđujući da nazivi domena ostanu nedvosmisleni. Takođe, očekuju da njihova mreža ubrza razrešavanje naziva za sve korisnike.

ORSN ima dva načina rada: Nezavisan i Baziran na ICANN-u. Baziran na ICANN-u predstavlja normalni način rada i podrazumeva dnevnu sinhronizaciju, osim što se uklonjeni TLD domeni ne uklanjaju iz ORSN root-a. Nezavisan režim rada se ne ažurira automatski i aktivira se „...kad god politička situacija u svetu – po našem mišljenju – učini ovaj korak neophodnim usled postojanja mogućnosti modifikacije i/ili pada ICANN-ove root zone...”<sup>23</sup>

#### **4.3 Budućnost DNS-a**

Odredjivanje najbolje budućnosti za ICANN i administraciju DNS-a nije pitanje na koje se lako može dati odgovor. Ali, u svakom slučaju, rasprave o ovoj temi su veoma važne i neophodno je da ih bude što više. Kako sve više ljudi u svetu postaje svesno *Internet*-a i uključuje *Internet* u svoje svakodnevne živote, kontrola koju ICANN ima nad DNS-om će imati sve veće implikacije.

---

<sup>23</sup> <http://www.orsn.org/faq.php>

## Zaključak

---

Običan korisnik *Internet*-a ne mora da zna puno o DNS-u, ali kad god se koristi *Internet* – koristi se i DNS. Svako slanje elektronske pošte ili surfovanje web-om oslanja se na Domain Name System. Zbog toga ova tema, a naročito bezbednost povezana sa njom, zasluži posebnu analizu.

Bezbednost sistema za adresiranje domena je velika tema – dovoljno velika da se o njoj napišu tomovi knjiga. Ovaj rad bi trebalo da predstavlja osnovno upoznavanje sa bezbednosnim pitanjima DNS-a, dok bi detaljno predstavljanje svih aspekata bezbednosti ovog sistema zahtevalo mnogo više prostora.

## Literatura

---

1. Albitz, Paul i Liu, Cricket – *DNS and BIND, Fourth Edition*, O'Reilly Publishing, april 2001.
2. Aitchinson, Ron – *Pro DNS and BIND*, Apress publishing, 2005.
3. Bellovin, Steven – *Using the Domain Name System for System Break-ins*, AT&T Bell Laboratories, 1995.
4. Farrel, Adrian – *Internet and its Protocols: A Comparative Approach*, Morgan-Kaufmann, 2004.
5. Kabelová, Alena i Dostálek, Libor – *DNS in Action*, Packt Publishing, 2006.
6. Vaughn, Randal i Evron, Gadi – *DNS Amplification Attacks, Preliminary release*, mart 2006.
7. RFC 1035 – *Domain Names – Implementation and specification*, The Internet Society, novembar 1987.
8. RFC 3833 – *Threat Analysis of the Domain Name System (DNS)*, The Internet Society, avgust 2004.
9. RFC 4033 – *DNS Security Introduction and Requirements*, The Internet Society, mart 2005.
10. RFC 4034 – *Resource Records for the DNS Security Extensions*, The Internet Society, mart 2005.
11. RFC 4035 – *Protocol Modifications for the DNS Security Extensions*, The Internet Society, mart 2005.
12. <http://www.dnssec.net/>
13. <http://www.icannwatch.org/>
14. <http://www.internetgovernance.org/>
15. <http://www.isc.org/>
16. <http://www.networkdictionary.com/>
17. <http://www.root-servers.org/>
18. <http://www.securityfocus.com/>
19. <http://www.wikipedia.org/>