РНИДС
Регистар националног интернет домена Србије

Фондација „Регистар националног интернет домена Србије“
Жоржа Клемансоа 18а/I, Београд | телефон: 011.7281.281
rnids.rs | рнидс.срб | kancelarija@rnids.rs

.rs .срб

Безбедан DNS систем

Децембар 2015.

Увод

Интернет је глобална рачунарска мрежа са неколико стотина милиона компјутера који међусобно комуницирају и размењују информације. За корисника, сваки од ових рачунара, или сервиса који они пружају, може бити идентификован преко јединственог имена – назива домена. Са друге стране, рачунари и елементи мреже, који омогућавају комуникацију преко Интернета, користе низове бројева – IP (Internet Protocol) адресе.

Сви корисници Интернета користе DNS (Domain Name System) да би се повезали са одговарајућим Интернет сервисом. Систем назива домена (DNS) је дистрибуирана база података о називима рачунара и сервиса на Интернету. Улога DNS-а је да корисницима омогући повезивање рачунара на Интернету, а да при томе корисници користе словне изразе који се лако памте. Многи од вас већ знају, или су чули, да рачунари међусобно комуницирају преко нумеричких IP адреса. Поједностављено, DNS је „IP именик" који називе рачунара и сервиса повезује са одговарајућим IP адресама (бројевима).

Основне карактеристике DNS система су:

- Да буде увек доступан
- Да буде поуздан
- Да буде брз
- Да буде флексибилан и проширив

DNS систем, као и многи други дистрибуирани рачунарски системи, има своје безбедносне слабости. Специфичност DNS система, његова глобална улога и намена да пружа услугу свим корисницима Интернета, утицала је да се приликом његовог развоја није придавала велика пажња његовој безбедности. Повећање броја корисника, нарочито повећање броја злонамерних корисника Интернета, последњих година је у фокус ставило безбедност DNS-а.

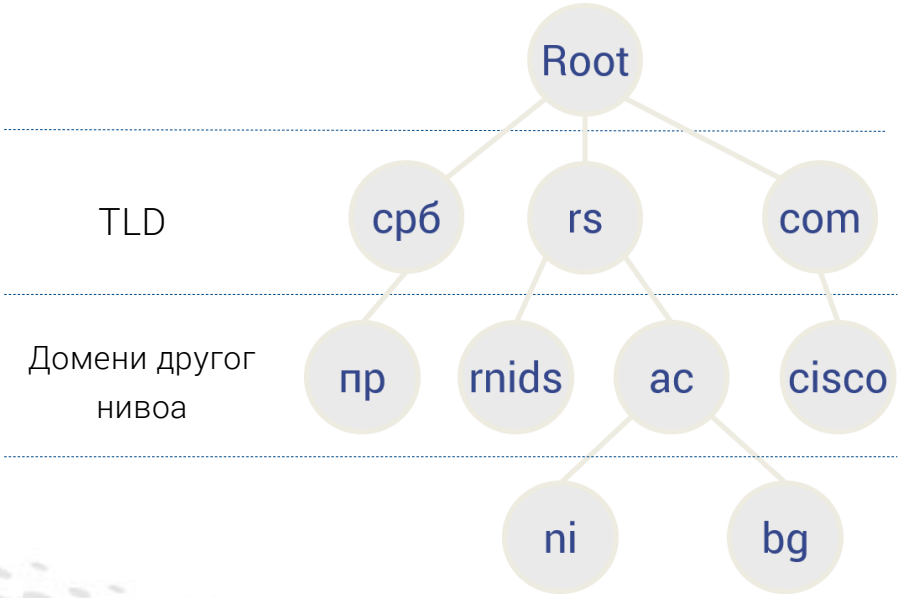
Међутим, и поред чињенице да је DNS један од кључних Интернет сервиса, њему се не придаје довољно пажње, пре свега од стране администратора и људи који су задужени за безбедност рачунарских система. DNS је веома моћан, свеприсутан и углавном игнорисан – то је веома опасна комбинација!

Циљ овог документа је да, корисницима представи могуће ризике и пружи кратка упутства за имплементацију и одржавање безбедног DNS система.

DNS сервис

Основни разлог постојања DNS-а је да омогући додељивање јединственог Интернет назива сервисима и рачунарима. Јасна корист од оваквог приступа је лако памћење Интернет назива сервиса, као што су веб стране или адресе електронске поште, уместо низа бројева садржаних у IP адресама тих сервиса. Осим тога, једнако важна је и чињеница да DNS омогућава одвајање назива сервиса од његове локације. Сервиси могу мењати своју физичку локацију потпуно транспарентно, а да при томе не мењају свој Интернет назив. Иста Веб страница се једног дана може налазити у Београду, а већ следећег у Токију или Мелбурну, а да корисници то и не примете. Промена се (осим пребацивања садржаја Веб странице на другу локацију) огледа једино у промени IP адресе у DNS запису Интернет назива тог сервиса.

Структура DNS-а се састоји од великог броја глобално распоређених рачунарских и комуникационих уређаја. На самом врху DNS структуре налазе се root сервери који садрже податке о доменима највишег нивоа (TLD), као што су: .rs, .ca, .se, .com, .net, итд. За сваку од TLD зона постоји DNS структура која садржи податке о доменима другог нивоа (.co.rs, rnids.rs, cisco.com,...). Аналогно, за сваку зону другог нивоа постоји структура са одговарајућим DNS подацима за ту зону...



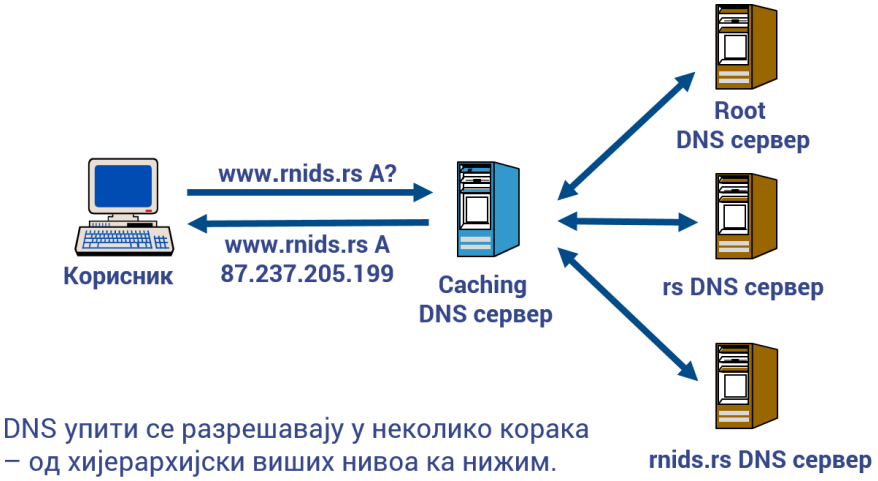
Како функционише DNS

Хајде да испратимо један DNS упит са рачунара корисника. Рачунар корисника зна адресу неког DNS сервера (то је најчешће DNS сервер Интернет провајдера или DNS сервер компаније). Када корисник у адресну линију веб претраживача укуца адресу

www.rnids.rs, рачунар ће послати упит том DNS серверу очекујући као одговор IP адресу веб стране РНИДС-а. Постоји велика шанса да DNS сервер вашег Интернет провајдера зна IP адресу www.rnids.rs јер су многи његови корисници пре вас имали исти захтев и DNS сервер је запамтио, или кеширао („cached" у DNS терминологији), и ваш рачунар ће одмах добити одговор. DNS кеш има двојаку улогу, да убрза налажење одговарајуће IP адресе за популарне Интернет сервисе, али и да смањи оптерећење глобалног DNS сервиса, јер упити не иду даље од првог DNS сервера који је познат вашем рачунару.

Ако Интернет адреса коју је корисник тражио, у овом случају *www.rnids.rs,* није позната вашем DNS серверу, или хијерархијским серверима за кеширање, упит који је његов рачунар послао ће стићи до самог корена глобалног DNS система, до root сервера, тачније, до једног од тринаест root сервера. Root сервери представљају посебан сет, хијерархијски највиших, DNS сервера који знају адресе ауторитативних DNS сервера за хијерархијски највише делове Интернет назива, тј. за део адресе са десна на лево до тачке. То је у нашем случају ,RS, али root сервери знају и IP адресе ауторитативних DNS сервера и за остале домене највишег нивоа, или TLD (Top Level Domain), као што су: com, net, org, edu, it, uk, se, de, срб, рф...

Када рачунар пошаље DNS упит, ваш DNS сервер ће, уколико му није позната адреса сервиса коју сте тражили, покушати да разреши (resolve) ту IP адресу и послаће упит једном од root сервера. Root сервер неће проследити одговор са IP адресом за *www.rnids.rs,* пошто му она није позната, већ ће DNS серверу (ресолверу) корисника послати листу DNS сервера који су ауторитативни за .RS. Тада ће DNS сервер корисника послати нови упит првом са листе DNS сервера који су ауторитативни за .RS, али ни од њега неће добити IP адресу за *www.rnids.rs*, већ листу ауторитативних DNS сервера за rnids.rs. DNS сервер поново шаље упит првом са листе ауторитативних DNS сервера за rnids.rs, и од њега добија IP адресу за *www.rnids.rs*, коју смешта у своју меморију (кешира је за случај да се у неком одређеном временском интервалу понови исти упит) и прослеђује је рачунару корисника. Треба напоменути да процес разрешавања IP адресе обично траје мање од 100 милисекунди и да крајњи корисник то време практично и не примети и није ни свестан колики је пут у ствари прешао његов DNS упит.



DNS упити се разрешавају у неколико корака – од хијерархијски виших нивоа ка нижим.

Сада и рачунар корисника зна IP адресу рачунара на коме се налази веб страна РНИДС-а и повезује се са веб сервисом на адреси 87.237.205.199 и у корисниковом веб претраживачу приказује тражену веб страну.

```
;; global options:  printcmd
.                16730  IN     NS     a.root-servers.net.
.                16730  IN     NS     l.root-servers.net.
.                16730  IN     NS     h.root-servers.net.
.                16730  IN     NS     b.root-servers.net.
.                16730  IN     NS     k.root-servers.net.
.                16730  IN     NS     f.root-servers.net.
.                16730  IN     NS     c.root-servers.net. …
;; Received 228 bytes from 82.117.194.2#53(82.117.194.2) in 12 ms
rs.              172800  IN     NS     l.nic.rs.
rs.              172800  IN     NS     k.nic.rs.
rs.              172800  IN     NS     h.nic.rs.
rs.              172800  IN     NS     g.nic.rs.
rs.              172800  IN     NS     f.nic.rs.
                  rs.              172800  IN     NS     d.nic.rs.
rs.              172800  IN     NS     b.nic.rs.
rs.              172800  IN     NS     a.nic.rs.
;; Received 460 bytes from 198.41.0.4#53(a.root-servers.net) in 18 ms
rnids.rs.          3600    IN     NS     ns1.nic.rs.
rnids.rs.          3600    IN     NS     ns2.rnids.rs.
rnids.rs.          3600    IN     NS     odisej.telekom.rs.
rnids.rs.          3600    IN     NS     ns1.rnids.rs.
;; Received 221 bytes from 194.146.106.114#53(l.nic.rs) in 0 ms
www.rnids.rs.        3600    IN     CNAME   web-server.rnids.rs.
web-server.rnids.rs.   3600    IN     A      87.237.205.199
rnids.rs.          3600    IN     NS     ns1.nic.rs.
rnids.rs.          3600    IN     NS     odisej.telekom.rs.
rnids.rs.          3600    IN     NS     ns1.rnids.rs.
rnids.rs.          3600    IN     NS     ns2.rnids.rs.
;; Received 262 bytes from 147.91.8.6#53(ns1.nic.rs) in 14 ms
```

Пример стандардног DNS упита

DNS сервис је једини централизован и хијерархијски организован сервис на Интернету. Уз то, DNS сервис се од свог настанка веома мало мењао и стога је разумљиво да DNS сервери, због свог значаја, представљају сталну мету злонамерних корисника Интернета. Циљеви нападача могу бити различити, од политичких и верских до материјалних, или једноставно деструктивних.

Обзиром да већину корисника не занимају технички детаљи рада DNS-а, овом сервису није посвећена довољна медијска пажња и едукација корисника о његовом значају, а како се у последње време показало, и на његове слабости које отварају нове могућности за злонамерно деловање на Интернету. Чак и многи рачунарски образовани корисници, па и систем администратори, сматрају DNS једноставним и досадним и не посвећују му довољно пажње коју, због свог значаја за функционисање Интернета, с правом заслужује.

Лоше конфигурисани и необезбеђени DNS могу бити искоришћени на различите начине, било као директни циљеви напада или као средство за напад на друге рачунарске системе било где у свету.

Последњих година у ударним вестима о нападима на системе великих банака, медијских кућа и водећих светских компанија, може се чути и прочитати да су нападачи користили лоше конфигурисане DNS сервере, или су на неки начин, у DNS системима, изменили IP адресе Интернет сервиса који су били мета напада.

Крајем марта, светом је прострујала вест да је на anti-spam провајдера Spamhaus извршен највећи DDoS (Distributed Denial of Service) напад у историји Интернета. За напад је оптужен холандски хостинг провајдер Cyberbunker чији су сервери за слање електронске поште претходно стављени на црну листу од стране Spamhausa. Како је могуће да један хостинг провајдер генерише саобраћај од преко 300Gb у секунди?

Према извештају Open Resolver Project у свету има више од 20 милиона лоше конфигурисаних и необезбеђених DNS сервера који могу бити искоришћени као „појачавачи“ напада, који генеришу многоструко већу количину података од иницијалне. Наиме, стандардни DNS упит је величине око 30 бајтова, док одговор који шаље DNS сервер може бити од 100 до 200 пута већи. Обично се DNS упит шаље путем UDP протокола, који не захтева успостављање двосмерне комуникације, што омогућава нападачима да се лажно представе (spoofing) и представе да упит долази са IP адресе жртве напада, а не са IP адресе са које је у ствари послат. DNS сервер у одговору шаље знатно већу количину података, али на IP адресу жртве. Ако узмемо у обзир да је један DNS сервер у стању да обради и пошаље одговоре на стотине хиљада DNS упита у свакој секунди, онда можете замислити колики саобраћај може произвести неколико стотина па и хиљада лоше конфигурисаних DNS сервера. Cloudflare је објавио да је у

прошлогодишњем нападу на њихову Интернет инфраструктуру, који је по обиму био знатно мањег интензитета од напада на Spamhaus, учествовало више од 65000 DNS сервера.

Пре нешто више од годину дана изведен је још један напад који се односи на DNS сервере, али другачије конципиран. Нападачу, који се представљају као Syrian Electronic Army (SEA), успели су да, користећи права приступа партнерске фирме за регистрацију Интернет домена, промене податке у DNS систему познатог аустралијског провајдера Melbourne IT и на тај начин преусмере Интернет кориснике великог броја познатих компанија, међу којима су New York Times, Washington Post, Financial Times, Twitter, и неке сервисе BBC-a, AP-a и Reuters-a, ка серверима који су под контролом нападача. Претпоставља се да је овај напад имао за циљ само политичку „видљивост“ на Интернету, али овај и слични напади могу имати много веће и озбиљније последице.

Преусмеравање Интернет саобраћаја, рецимо New York Times-a, значи и могућност преусмеравања електронске поште на сервере који су контролисани од стране нападача, а самим тим и отворен приступ електронској комуникацији путем и-мејла. У случају Melbourne IT таква промена је била брзо примећена, али је веома вероватно да би такав сценарио код мање опрезних DNS оператера био откривен тек данима, а можда и месецима касније.

Познато је да су чести случајеви преусмеравање корисника сервиса на Интернет локације, које контролишу нападачи и које се по свом изгледу и садржају не разликују од оригиналних сервиса којима је корисник желео да приступи. Много је начина за реализацију оваквих напада, али је измена DNS записа, сервиса банака, Интернет продавница и других сервиса где се од корисника тражи да унесу осетљиве податке о свом идентитету или бројеве кредитних картица И банковних рачуна, чест и веома ефективан начин да се у кратком временском року „превари“ велики број корисника.

Најчешћи тип напада на DNS сервис су:

- DoS и DDoS напади
- Употреба DNS сервера за амплифицирани DDoS напад на друге интернет сервисе
- Пресретање и измена DNS пакета (man in the middle)
- "Тровање кеша" (cache poisoning)
- Измена DNS записа и зонског фајла

DoS и DDoS

Интернет је глобална мрежа на коју су повезане милијарде различитих уређаја и који омогућава њихову брзу размену података и информација. И поред те чињенице Интернет ипак има ограничене ресурсе и њихова потрошња (искоришћеност) није бесконачна. Интернет линкови, капацитети мрежних уређаја, рачунарски процесори и уређаји за складиштење података имају своје лимите који могу бити искоришћени као мета напада.

Веома честа врста напада су инциденти у којима су делови система лишени одговарајућих ресурса који су потребни за њихов нормалан рад. Користећи рањивост стандардних Интернет протокола нападачи могу да покрену напад ускраћивања сервиса, Denial of Service (DoS) напади, чији је циљ да онемогуће систем да пружа услуге корисницима. Иако DoS напади најчешће не доводе до крађе или губитка значајних података, они ипак жртву напада могу коштати много времена и новца.

Најчешће мете оваквих напада су веб сервери банака, медијских кућа, владиних институција или Интернет трговина, али су такође чести и напади на DNS инфраструктуру и сервисе електронске поште. DoS напади се извршавају тако што нападач шаље велику количину података ка жртви напада, или слањем информација које могу проузроковати пад система. У оба случаја, нападач спречава легитимне кориснике система да користе сервисе или ресурсе које очекују.

DoS напад је злонамерни покушај једне особе или групе људи да проузрокује напад на систем жртве и на тај начин ускрати услугу клијентима. Када овакав покушај потиче са једне локације, он представља DoS напад. С друге стране, додатни облик DoS напада је Distributed Denial of Service (DDoS) напад за који је карактеристично да вишеструки системи, са различитих локација, синхронизовано врше DoS напад на јединствену мету напада. Суштинска разлика је у томе да је, уместо напада са једне локације (DoS), систем жртве нападнут са много локација одједном. Дистрибуција система са којих се напад извршава даје нападачу много предности:

- Нападач може да користи значајне ресурсе за реализацију веома озбиљног напада
- Скоро је немогуће детектовати локацију одакле напад долази јер су ти системи дистрибуирани широм света
- Много је теже блокирати нападе који долазе са више система и локација
- У пракси је скоро немогуће идентификовати правог нападача јер је он најчешће сакривен иза много (најчешће) компромитованих система.

Савремени системи за заштиту имају механизме за заштиту од већине DoS напада, али због специфичности DDoS напада он се и даље сматра озбиљном претњом. Уколико је DDoS напад изведен са довољном количином ресурса није га могуће успешно зауставити.

Покретање DDoS напада захтева изградњу мреже рачунара који су под контролом нападача (такозвани botnet). За ширење злонамерног кода и „изградњу" botnet мреже користе се различити механизми, али је суштина у злоупотреби непажње Интернет корисника који из незнања или ниподаштавања опасности остављају своје системе незаштићене од потенцијалних неовлашћених упада или ширења злонамерног кода. Многи корисници Интернета били су саучесници DDoS напада, а да тога нису били свесни. Стога је веома битно водити рачуна да је антивирусни програм функционалан и са најновијом базом вируса, да су све исправке (печеви) везани за сигурност система инсталирани и да су сви могући приступи системима добро обезбеђени.

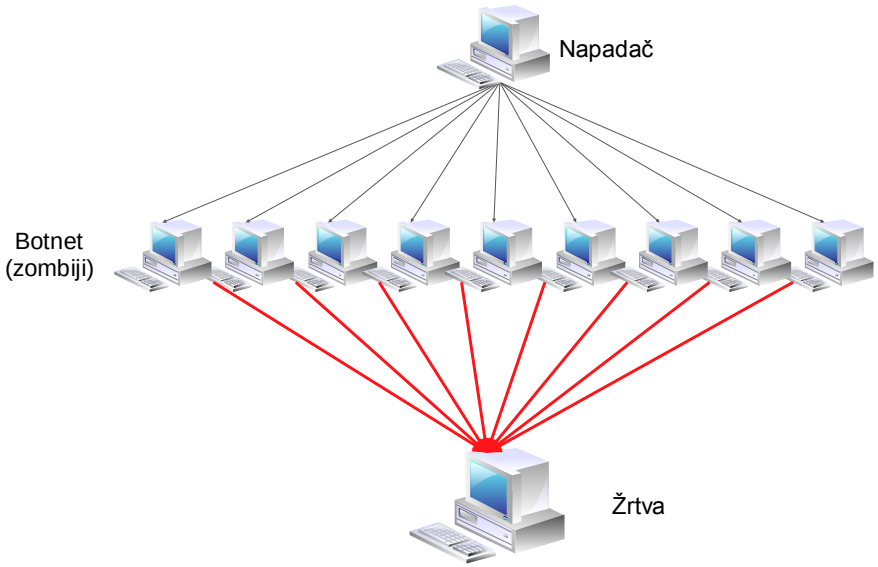
Уколико ове сигурносне мере нису испоштоване лако се може десити да отварањем сумњиве и-мејл поруке или посете веб страни која садржи злонамерни код, ваш рачунар постане „зомби", тј. део botnet мреже која је под контролом нападача.

Већ је поменуто да се DDoS напад реализује када се велики број компромитованих машина, инфицираних злонамерним кодом, синхронизовано, под контролом једног нападача, користи за исцрпљивање ресурса система жртве и ускраћивање услуга корисницима. Постоје две основне врсте DDoS напада:

- Стандардни DDoS напади,
- Рефлектовани DDoS (DRDoS) напади.

У стандардном DDoS нападу нападач шаље наредбу „армији зомбија" (botnetu), коју је креирао ширењем злонамерног кода, и покреће напад на систем жртве. Сваки агент (зомби), користећи своје рачунарске и мрежне ресурсе, почиње да шаље велики број пакета ка систему жртве, преплављујући (енглески flooding) његове ресурсе.

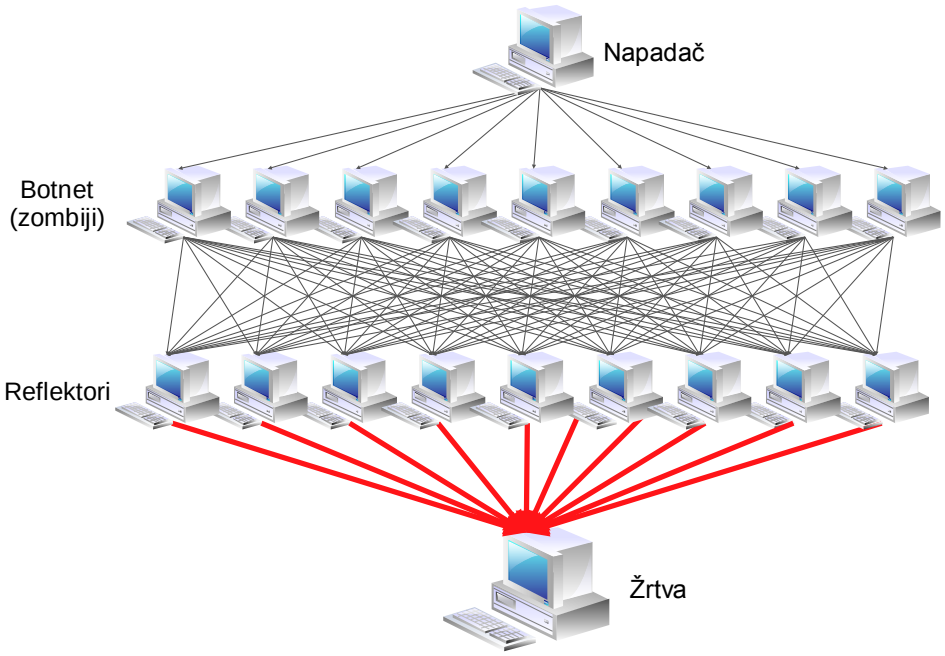
У већини DDoS напада користе се лажне (spoofed) IP адресе како жртва не би могла да прати прави извор напада, али и из разлога смањења могућности да жртва успешно филтрира злонамерни саобраћај на фајерволу (firewall).



DDoS напад

За разлику од стандардног DDoS напада, рефлектовани или DRDoS напади се изводе тако што армија зомбија шаље велики број пакета са, лажном ИП адресом жртве, на системе који пружају легитимну услугу (рефлекторе), захтевајући да одговор пошаљу ка систему жртве. Оваква врста напада је много деструктивнија од стандардног DDoS напада јер је могуће „ангажовати“ много више рефлекторских система него што има зомбија и на тај начин знатно повећати количину саобраћаја усмерену ка систему жртве.

Последњих неколико година DNS системи се користе за специфичну врсту рефлекторских напада, а то су појачани DDoS (amplified DDoS) напади. У ранијим текстовима је поменуто да су DNS упити много мањи (и до неколико стотина пута) од одговора које шаљу DNS сервери. Лоше конфигурисани DNS сервери који дозвољавају јавну рекурзију (свима шаљу одговоре и на DNS упите за које нису ауторитативни) били су коришћени у неколико највећих DDoS напада. Веома је битно да администратори система провере своје DNS сервере и конфигуришу их тако да DNS одговоре за које нису ауторитативни шаљу само одређеној групи корисника. Недавна анализа RNIDS-а, у сарадњи са RCUB-ом, показала је да скоро 10000 DNS сервера, који се користе у .RS и .СРБ доменским просторима, дозвољавају јавну рекурзију. У свету има више од 20 милиона таквих сервера.



Рефлектовани DDoS напад (DRDoS)

До данас није развијен сигуран метод који омогућава успешну одбрану од DoS/DDoS напада. Нападачи много брже проналазе нове и напредније методе за реализацију напада, него што ефикасни одбрамбени системи могу да буду имплементирани. Иако су многе компаније које улажу десетине милиона долара на безбедност система биле изложене успешним DDoS нападима, то не значи да не треба ништа радити на повећању сигурности система и превентивно деловати у циљу ублажавања ефеката напада.

Постоје три нивоа заштите од DDoS напада: ниво корисника; ниво трансмисије; и ниво система.

- На нивоу корисника треба радити на едукацији и подизању свести о потенцијалним опасностима, не само по системе самих корисника, већ и о могућностима да незаштићени системи могу бити искоришћени за напад на друге системе на интернету.

- Имплементација филтера који спречавају пренос пакета података са лажном IP adresom (Network Ingress Filtering RFC 2827) омогућила би детекцију извора напада и ефикаснију заштиту далеко од система жртве. Такође, добра сарадња са Интернет провајдерима и њиховим над-провајдерима на филтрирању нежељеног саобраћаја обезбедила би несметан рад система жртве. Када су у питању напади који за циљ имају загушење комуникационих линкова, ограничавање саобраћаја и филтрирање пакета далеко од система жртве је и

јединi ефикасан начин за умањење или елиминисање ефеката DoS/DDoS напада.

- Коначно, на нивоу самог система потребно је обезбедити довољно ресурса за кључне сервисе које систем пружа корисницима. Такође, могуће имплементирати ефикасне системе за филтрирање и ограничавање нежељеног саобраћаја који представља опасност за несметан рад система.

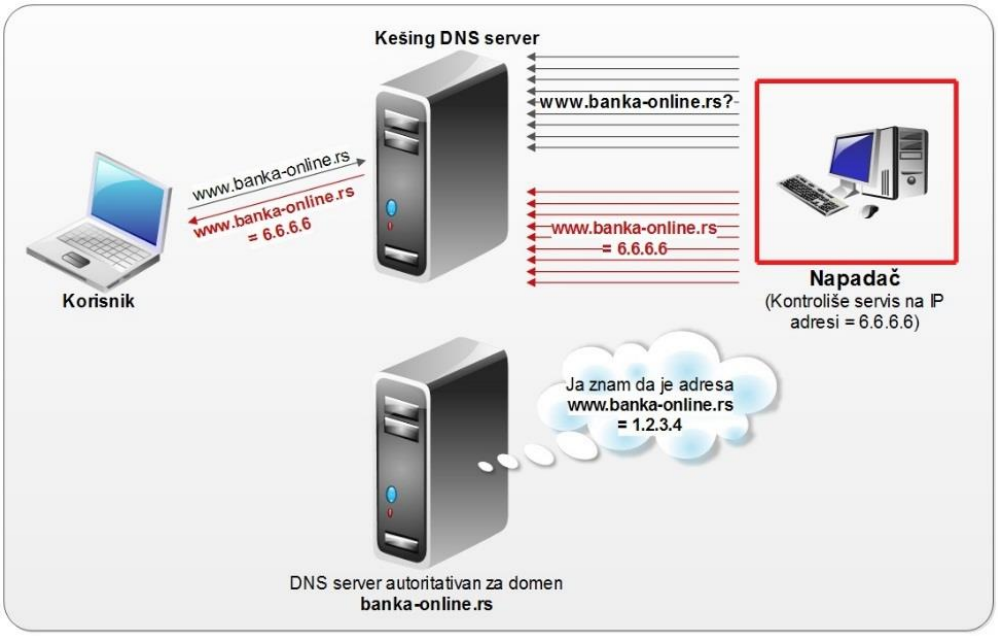
Cache poisoning напади

У највећем броју случајева корисници умрежених рачунара користе DNS сервис своје компаније или интернет провајдера. Локални DNS сервери имају превасходни задатак да побољшају и убрзају процес разрешења DNS упита (упаривање назива Интернет сервиса са одговарајућом IP адресом рачунара који пружа тражени сервис) кроз „памћење“ раније добијених одговора на DNS упите (caching). Раније су поменути значај DNS сервиса и могуће последице по кориснике уколико је овај сервис недоступан или му се проследи погрешна информација о IP адреси траженог Интернет сервиса.

Одавно је позната рањивост DNS система везана за измену раније запамћених одговора на DNS упите. Оваква врста злонамерног деловања је позната као „тровање кеша“ (cache poisoning). Ова техника може бити коришћена за преусмеравање корисника на интернет сервисе које контролише нападач, а да сам корисник није свестан да услуга или садржај нису аутентични.

Суштина ове врсте напада је у томе да нападач својом активношћу измени запамћен „кеширан“ садржај на кешинг DNS серверу. Успешно изведен „cache poisoning“ Напад на један DNS сервер може имати негативан утицај, не само на директне кориснике сервиса, већ и на хијерархијски ниже DNS сервере који користе нападнути DNS сервер за разрешавање DNS упита.

Нападач шаље велики број упита за, одабрани домен ка DNS серверу који је нападнут и истовремено шаље лажне одговоре представљајући се као ауторитативни DNS сервер за тај домен. Уколико одговор од нападача стигне пре одговора ауторитативног сервера, DNS сервер ће запамтити погрешан одговор и у периоду важења (TTL – time to live) запамћеног DNS записа, прослеђивати га корисницима као валидан.



Cache poisoning напад

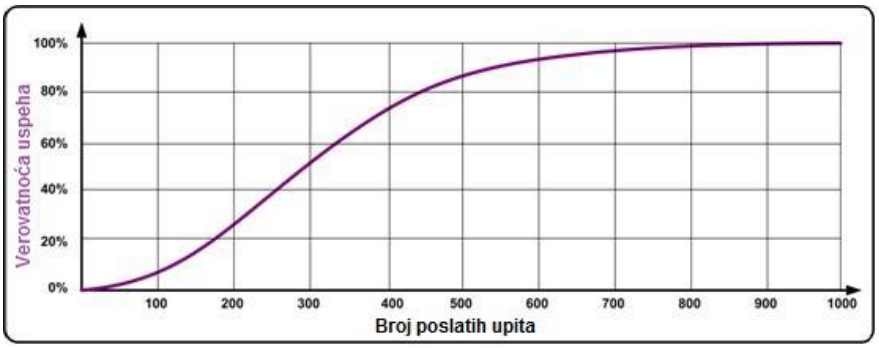
Да би напад био успешан нападач мора да пошаље велики број DNS упита DNS серверу који напада и да у исто време шаље једнак број лажних одговора. Нове генерације DNS сервера као валидан DNS одговор прихватају одговор који у себи садржи тачан број трансакције (transaction ID) и број порта који се генерише методом случајних бројева.

Концепт успешно изведених напада базиран је на теореми из теорије вероватноће познатом као „парадокс рођендана“ ("Birthday Paradox"), која каже да је вероватноћа, да у групи од 23 људи двоје или више њих има рођендан истога дана, већа од 50%. Општа дефиниција теореме каже да ако су улазне вредности неке функције бројеви добијени методом случајних бројева и као резултат даје једну од и једнако вероватних вредности, тада ће се иста вредност у резултату појавити након $1{,}2\sqrt{\mathrm{i}}$ понављања (парадокс рођендана је специјални случај теореме где је i=365).

Број трансакције је 16 битни број што значи да нападач слањем n одговора, на један упит, има n/65536 шансе да погоди тачан број трансакције. Међутим, уколико применимо описану теорему на случајно генерисани број трансакције и узмемо у обзир чињеницу да DNS сервери генеришу вишеструке упите ка ауторитативном DNS серверу за исти домен, могуће је знатно повећати вероватноћу да лажни одговор који шаље нападач садржи тачан број трансакције. Вероватноћа успешног погађања броја трансакције рачуна се по формули:

$$Verovatnoća = 1 - (1 - \frac{1}{t})^{\frac{n\,(n-1)}{2}}$$

Где је t број могућих вредности (у нашем случају 65536), а n је број упита и лажних одговора које нападач шаље. За разлику од стандарног рачунања, где је вероватноћа успеха n/65536 (за n=700 послатих одговора вероватноћа би била 1,07%), употребом „birthday attack“ методе, 700 послатих упита и исто толико лажних одговора даје скоро 100% вероватноћу да ће нападач погодити број трансакције. Зависност вероватноће успеха од броја парова упит-одговор дата је на графику. Видимо да са само 300 послатих упита и лажних одговора (ово не захтева посебне рачунарске ресурсе и интернет конекцију) нападач има 50% шансе за успех.



Налажење тачне IP адресе сервера је лако: нападач зна мету напада и познате су му адресе ауторитативних сервера за домен чији запис покушава да лажира. Остаје најтежи задатак да нападач нађе одговарајући порт који се подудара са бројем порта који нападнути DNS сервер шаље у свом упиту ка ауторитативним DNS серверима за тражени домен. Иако се број порта генерише методом случајног броја, DNS сервер ће најчешће употребити исти порт за упите који долазе од истог клијента. Ако нападач има приступ неком од ауторитативних DNS сервера за било који домен, он ће најпре DNS серверу који напада послати упит за домен за који је ауторитативан сервер који он контролише, а затим употребити исти тај порт у лажним одговорима за домен чије погрешне податке покушава да убаци у меморију нападнутог сервера. Погледајмо секвенцу упита за различите називе домена од стране истог клијента:

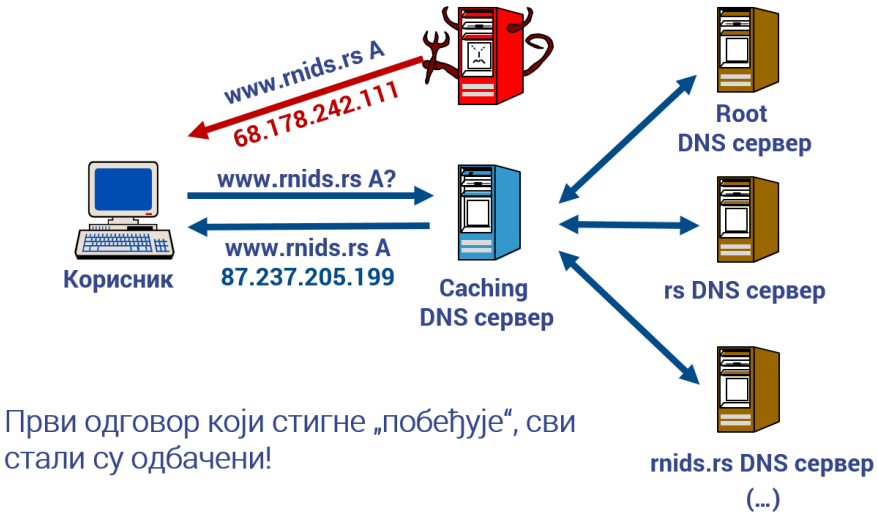
```
10:54:12.423228 192.168.1.2.33748 > 66.218.71.63.53: 21345 [1au] A? www.yahoo.com. (42) (DF)
10:54:21.313293 192.168.1.2.33748 > 216.239.38.10.53: 53735 [1au] A? www.google.com. (43) (DF)
10:54:27.182852 192.168.1.2.33748 > 149.174.213.7.53: 19315 [1au] A? www.netscape.com. (45) (DF)
10:54:43.252461 192.168.1.2.33748 > 66.35.250.11.53: 43129 [1au] A? www.linux.com. (42) (DF)
```

Све линије имају исти број порта (33748) иако су упити били везани за различите домене. Нападачу сада једино преостаје да његови лажни одговори стигну пре одговора који је послао ауторитативни DNS сервер за домен чије погрешне податке покушава да утисне у меморију нападнутог DNS сервера. Нападачи најчешће при реализацији овакве врсте напада преплављују ауторитативне сервере огромним бројем

упита како би их успорили или потпуно онемогућили да валидан DNS одговор стигне пре лажног.

Успешно уписивање лажних DNS податке у меморију кешинг сервера отвара низ различитих могућности за злоупотребу. Преусмеравање веб саобраћаја на веб стране које контролише нападач и које изгледају потпуно исто као оригинал или преусмеравање и-мејл порука ка серверу нападача.

Посебно је опасна могућност преусмеравања целокупног интернет саобраћаја, такозвани „Man in The Midle“ MTM напад, где нападач пресреће комплетну комуникацију нападнутог домена и има приступ и могућност да мења садржај порука које две стране размењују.



Једноставан MTM напад

Иако су овакве врсте напада познате од почетка 90тих већина DNS сервера који су данас у функцији још увек је рањива и нема адекватну заштиту. Најновије верзије DNS софтвера имају повећан ниво заштите од „cache poisoning“ напада. Такође, веома је битно да DNS сервери буду конфигурисани тако да DNS упите на које ће одговарати примају само од одређене групе корисника, а не од било ког корисника на Интернету. У овом тренутку највиши ниво заштите DNS сервиса, од овакве врсте напада, представља DNSSEC (сигурносна екстензија за криптовану проверу аутентичности DNS одговора).

DNSSEC

У тренутку када је DNS систем креиран није се много размишљало о његовој безбедности. Данас, када је преусмеравање корисника ка нежељеним интернет локацијама и сервисима постало реалност, мора се размишљати о томе да ли је добијени одговор аутентичан и да ли је добијен од ауторитативног сервера. Из тог разлога креирано је безбедносно проширење DNS сервиса, познатије као DNSSEC (DNS Security Extension), које практично елиминише могућност „man in the middle" напада.

DNSSEC је стандард који модификује DNS записе и протоколе DNS-а у циљу повећања безбедности трансакција између DNS ресолвера и ауторитативног DNS сервера и омогућава:

- Потврду извора: Ресолвер може да одреди да ли одговор потиче од ауторитативног DNS сервера за одређену зону.
- Потврду интегритета: Ресолвер може да одреди да ли је одговор мењан у току преноса.
- Аутентично порицање постојања: Ресолвер може да потврди да је одређени упит неразрешив, ако не постоји DNS запис ресурса на ауторитативном серверу.

Како то ради у пракси?

Да би зона била DNSSEC потписана креатор зоне генерише пар кључева који представља основу за PK шифровање (Public Key encryption). Приватни кључ се користи за шифровање садржаја поруке, а поруку је могуће дешифровати јавним кључем који је јавно доступан кроз DNSKEY запис у зонском фајлу. Приватни кључ се безбедно чува на уређају који се користи за потписивање зоне и није га могуће генерисати на основу јавног кључа и шифрованих података.

Сваки пут када се креира зонски фајл за DNSSEC потписану зону, сви DNS записи (A, MX, CNAME, итд.) дигитално се потписују новим типом DNS записа, који је креиран за DNSSEC и зове се RRSIG (resource record signature). RRSIG представља дигитални потпис који се формира узимањем hash-а одређеног скупа записа у зони и његовом шифровањем уз помоћ приватног кључа из комплета криптографских кључева администратора те зоне. Овако креиран потпис се шаље DNS ресолверу приликом сваког DNS упита. Ресолвер затим, генерише hash RRset дела одговора и упоређује га са hash-ом добијеним из RRSIG дела одговора и на тај начин потврђује или негира интегритет и аутентичност добијених DNS информација.

Да би били сигурни да је одговор стигао од аутентичног извора потребно је успоставити ланац поверљивости. Када је зона потписана, та информација се објављује у облику DS записа у хијерархијски вишем нивоу DNS структуре и представља тачку делегирања између зона вишег нивоа и зона нижег нивоа која се може потврдити. Да би потврдио DNSKEY зоне нижег нивоа, ресолвер преузима одговарајући DS, RRSIG(DS) и DNSKEY зоне вишег нивоа.

DS запис се налази на хијерархијски вишем нивоу у DNS структури и преставља одговарајући део кључа за потписивање зоне (ZSK) и потврђује да је зона на нижем хијерархијском нивоу потписана, а подаци из DS записа се користе за потврду DNSKEY података зоне нижег нивоа. На овај начин, потписани DS функционише као "сертификат" који се ауторитативно испоручује из зоне вишег нивоа и везује зону нижег нивоа за свој DNSKEY. DNS сервер из зоне вишег нивоа постаје, практично, "поуздано треће лице", које омогућава размену DNS информација између ресолвера и зоне нижег нивоа. Низ оваквих делегираних односа формира ланац поверљивости, који представља путању коју ресолвер може да прати од јавног кључа (тј. поузданог полазишта – trust anchor), а то су DNS root сервери. На крају, следећи безбедан (NSEC) запис, повезује потписане ресурсе, омогућавајући ресолверу да претражује зонски фајл и да одреди да ли запис за одређени домен постоји у зонском фајлу.

DNSSEC користи два типа кључева: кључеви за потписивање зоне (Zone Signing Keys – ZSK) и кључеви за потписивање кључева (Key Signing Keys – KSK). Тајни ZSK кључ се користи за потписивање и потврду индивидуалних записа у зони и његов одговарајући јавни кључ се објављује у виду DNSKEY записа. Јавни KSK кључ се такође појављује као DNSKEY запис, али се његов тајни кључ користи само за потписивање DNSKEY записа зоне.

Два различита кључа се користе из безбедносних разлога. Опште правило у криптографији је да што се више података шифрује одређеним кључем, опасност да се кључ сазна постаје све већа. У овом случају у питању је тајни кључ. У DNS-у се тај кључ користи за потписивање велике количине података јер свака промена у зони захтева поновно потписивање. Што је зона већа, то има више података који су доступни за криптоанализу. Из тог разлога, пракса је да се ЗСК кључеви мењају релативно често. Када би се користио само један кључ, сваки пут када би се он мењао, било би неопходно слати DNSKEY хијерархијски вишој зони како би се у њој заменио и поново потписао DS запис за ту зону. Да би се ово избегло, користе се два одвојена типа кључева, и хијерархијски вишу DNS зону је потребно контактирати само при промени KSK кључева, што се чини релативно ретко (њиме се потписује врло мало података). Одржавање јаке безбедности система овим постаје лакше и брже.

Наравно, DNSSEC заштита не зависи само од тога да ли је нека DNS зона потписана. Једнако је важно да локални DNS ресолвери (најчешће DNS сервери Интернет провајдера) буду конфигурисани тако да верификују DNSSEC записе.

Када DNS ресолвер код кога је омогућена DNSCEЦ верификација пошаље упит хијерархијски вишем DNS серверу за одређени домен, у одговору ће добити информацију да ли је тај домен дигитално потписан. Уколико јесте, ресолвер ће од ауторитативног сервера прихватати само дигитално потписане одговоре, а сваки други ће бити одбачен.

Повећање безбедности DNS система на овај начин, важно је не само крајњим корисницима већ и пружаоцима услуга, нарочито оним који се баве финансијским трансакцијама на Интернету, као што су банке, осигуравајућа друштва, Интернет продавнице…

Дигитално потписивање домена знатно смањује могућност да корисници буду преусмерени ка лажним интернет садржајима и самим тим повећава њихово поверење и омогућава раст и развој интернет пословања.

Како заштити себе и друге

Већина корисника не разуме DNS, пре свега, јер им није ни потребно да разумеју како ради да би користили Интернет. DNS једноставно функционише! И баш зато што DNS „једноставно функционише“, нико му не посвећује пажњу коју DNS , као један од основних сервиса на Интернету заслужује. Ако на пример неки од Интернет сервиса (веб, мејл, FTP…) не ради, има за последицу недоступност тог сервиса. Са друге стране, ако DNS сервис стане, све остало ће стати. Осим тога, неадекватна конфигурација DNS сервиса може да угрози друге кориснике Интернета.

Због свега тога треба:

Редовно проверавати DNS рекорде у родитељској зони

Нико није имун на грешке или нападе злонамерних корисника, па ни оператери root зоне, TLD оператери или Интернет провајдери. Због тога је неопходно редовно проверавати исправност DNS записа у родитељској зони (хијерархијски виша DNS зона која садржи податке о вашим DNS серверима).

Такође је веома битно водити рачуна о истеку валидности домена. Подаци за домен који је истекао се не налазе у зони DNS оператера код кога је домен регистрован, и

самим тим упити за такав домен неће бити разрешавани. То за последицу има недоступност сервиса, али може бити искоришћено и за злонамерне активности.

Редовно ажурирати софтвера (инсталација нових верзија DNS сервера и надградњи)

Злонамерни корисници проналазе нове начине за злоупотребу. Због тога је важно стално пратити и имплементирати све допуне (печеве) и нове верзије софтвера које у себи садрже решења за безбедносне пропусте који су у међувремену откривени.

Омогућити разрешавање DNS упита само за кориснике вашег система

DNS open resolver је DNS сервер који дозвољава свим клијентима, па и онима који нису део његовог административног домена да користе тај сервер за слање DNS упита и добијање одговора од њега и за зоне за које тај сервер није ауторитативан. Обезбедите свој сервер и омогућите разрешавање неауторитативних одговора само групи корисника којој је тај сервер намењен.

Активирати „Response Rate Limiting“ (RRL) на ауторитативним серверима

Задатак DNS сервера је да одговоре за зоне за које су ауторитативни пружају свима. Због тога и они могу бити искоришћени за DDoS и DRDoS нападе на рачунаре и системе других корисника. „Response Rate Limiting“ (RRL) омогућава ограничење броја одговора које DNS сервер шаље. Критеријуми за ограничење могу бити različiti (po IP адреси, типу упита, броју истих одговора…). Активирањем RRL-а ваш сервер постаје мање атрактиван за нападе на друге системе.

Забранити саобраћај адресама које нису део вашег система (SAV –Source Address Validation)

Слање DNS упита са лажном IP адресом не угрожава само ваш DNS сервис, већ може нанети огромну штету корисницима ка којима је одговор вашег DNS сервера преусмерен. Контролом саобраћаја, тј. Филтрирањем IP адреса које нису део вашег система повећавате општу безбедност на Интернету.

Валидирати DNSSEC

Криптовање података је веома битно за повећање безбедности и поузданости DNS-а. Потписивање зоне је само један од корака за постизање жељеног нивоа поузданости DNS система. Да би сигурност DNS сервиса била потпуна, неопходно је да и сви ресолвери imaju aktiviranu проверу дигиталног потписа за податке које добијају од DNS сервера који су ауторитативни за дигитално потписане зоне.