

DNS: nepotrebne bogon liste



Prije nekoliko godina smo na Portalu za sistemce pisali o problemu **bogon** ACL listi (*Access Control List*) u konfiguraciji BIND DNS poslužitelja, koje su onemogućavale pristup nekim dijelovima weba, odnosno internet prostora. Podsjetimo se što su zapravo bogon liste.

Bogon rasponi IP adresa u ACL listama su rasponi IP adresa koji još nisu dodijeljeni ni jednoj mreži, te stoga mogu izvršno poslužiti za DoS napade. Zbog toga postoje filtri u DNS servisu i routing listama jer ni jedan paket ne bi smio doći s tih adresa. No, ove IP adrese se povremeno (svakih nekoliko mjeseci, u prosjeku svaka 4 mjeseca) dodjeljuju novim institucijama, odnosno ISP-ovima. Tako se može dogoditi da uslijed neažurnosti lista, koje nastavljaju blokirati novododijeljene raspone IP adresa, dio internet prostora postane nedostupan.

Dva su načina rješavanja ovog problema: uopće ne rabiti bogon liste, ili ih redovito osvježavati. Prvi način je jednostavniji, no otvara mogućnost napada izvan naše mreže. Drugi način traži veći angažman, jer automatiziranog osvježavanja nema. Nakon konzultacija sa kolegama koji se bave sigurnošću, možemo reći da je opasnost od napada iz bogon raspona zanemariva. Također, možemo dodati da je svakog dana opasnost zapravo sve manja, jer se gotovo svakodnevno smanjuje slobodni IPv4 adresni prostor, a time i manevarski prostor eventualnim napadačima.

Ukoliko Vam je slučajno zaostala u konfiguraciji, bogon listu možete pronaći u datoteci `/etc/bind/named.conf` (možda je odvojena u neku drugu datoteku u `/etc/bind` direktoriju, provjerite). Trebate ju jednostavno zakomentirati ili obrisati:

```
// acl "bogon" {  
// 0.0.0.0/8;  
// 1.0.0.0/8;  
// 2.0.0.0/8;  
// 5.0.0.0/8;  
// 7.0.0.0/8;  
// 10.0.0.0/8;  
// };
```

U "options" bloku još treba zakomentirati "blackhole" parametar:

```
// blackhole {  
// bogon; };
```

```
// };
```

Nakon toga treba restartati BIND sa:

```
# /etc/init.d/bind9 restart
```

Radi potpunosti, spomenut ćemo neke web stranice koje se bave bogon listama i uvijek imaju najsvježije popise adresa u slučaju da i dalje želite imati aktivne bogon liste.

Web site koji se bavi problematikom bogon lista i nudi download osvježene bogon liste. Tu je i mailing lista s najnovijim promjenama u bogon listi:

<http://www.cymru.com/Bogons/> [1]

Tekstualna bogon lista spremna za ubacivanje u vaš DNS sustav ili router listu:

<http://www.cymru.com/Documents/bogon-bn-nonagg.txt> [2]

Alat za provjeru dostupnosti pojedinih raspona IP adresa:

<http://www.ris.ripe.net/debogon/> [3]

Potpuna lista Ipv4 adresnog prostora:

<http://www.iana.org/assignments/ipv4-address-space> [4]

- [Logirajte](#) [5] se za dodavanje komentara

uto, 2008-10-21 13:10 - Željko Boroš**Kuharice:** [Linux](#) [6]

Kategorije: [Operacijski sustavi](#) [7]

Vote: 0

No votes yet

Source URL: <https://sysportal.carnet.hr./node/444>

Links

- [1] <http://www.cymru.com/Bogons/>
- [2] <http://www.cymru.com/Documents/bogon-bn-nonagg.txt>
- [3] <http://www.ris.ripe.net/debogon/>
- [4] <http://www.iana.org/assignments/ipv4-address-space>
- [5] <https://sysportal.carnet.hr./sysportallogin>
- [6] <https://sysportal.carnet.hr./taxonomy/term/17>
- [7] <https://sysportal.carnet.hr./taxonomy/term/26>