Loša konfiguracija DNS-a omogućila DDoS napad na Spamhaus

Prema vijestima koje prenose svjetski mediji, prošlog je tjedna švicarska organizacija Spamhaus bila žrtva najvećeg dosad zabilježenog DDoS napada. Napadači su, koristeći botnete, proizveli promet od 300 GB po sekundi, koji je onemogućio rad Spamhausovim serverima. Raniji su napadi generirali promet između 4 i 10 GBps.

Napadi umjerenog intenziteta počeli su 19. ožujka, ali je količina paketa s vremenom rasla do te mjere da je uzrokovala zagušenja prometa širom EU. Kao povod napadu spominje se stavljanje nizozemske organizacije Cyberbunker na crnu listu spamera. Cyberbunker je smješten u napuštenom NATO bunkeru i spreman je pružiti hosting progonjenim domenama, poput Piratebaya i Wikileaksa, pa vjerojatno i kojekakvim spamerima.

Napad je izveden pomoću DNS servisa, koristeći takozvani “DNS amplification attack”. DNS serverima su slani upiti sa "spoofanom" IP adresom, pa su slali odgovore Spamhausu.

Organizacija Open DNS Resolver Project [1] već godinama apelira da se koristi sigurnija konfiguracija DNS servisa. Oni procjenjuju da je u svijetu oko 27 milijuna DNS servera konfigurirano na način da odgovara svima, a ne samo računalima unutar domene za koju je DNS servis postavljen. To su takozvani "open resolvers". Svega je 100.000 takvih DNS servera iskorišteno za napad na Spamhous, ali je to bilo dovoljno da se dogodi DDoS napad koji je po količini prometa usmjerenog na žrtvu ocijenjen kao najjači dosada.

Stručnjaci za informacijsku sigurnost nadaju se da će ovaj incident skrenuti pažnju vlasnika domena i da će se potruditi ispraviti konfiguracijske greške.

Pogledajmo kako možemo spriječiti da se naši DNS serveri iskoriste za ovakve napade. Podrazumijevana konfiguracija bind-a u verziji 9.4.1. bila je ovakva:

```
options {
     ...
     allow-recursion { any; };
     allow-query { any; };
     allow-query-cache { any; };
     ...
 };
```

Dakle, odgovara se svima koji pošalju upit.

Ono što treba napraviti jest unijeti pristupnu listu koja osigurava "punu uslugu" samo za računala iz mreža koje DNS poslužuje, nazvane "trusted":

```
acl "trusted" {
     192.168.0.0/16;
     161.53.xxx.0/24;
     localhost;
     localnets;
};
options {
```

```
    ...
    allow-query { any; };
    allow-recursion { trusted; };
    allow-query-cache { trusted; };
    ...
};
```

Time su rekurzivni upiti dozvoljeni samo klijentima iz naše mreže. CARNetov paket bind donosi sigurnu konfiguraciju, no ne škodi iskoristiti ovu prigodu da bi još jednom provjerili da li je vaš DNS server "otvoren".

ned, 2013-03-31 10:28 - Aco Dmitrović**Vijesti:** Događanja [2]
Kategorije: Sigurnost [3]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1241

Links
[1] http://openresolverproject.org
[2] https://sysportal.carnet.hr/taxonomy/term/43
[3] https://sysportal.carnet.hr/taxonomy/term/30