Amavis: Što u logovima znači "Hits: -"?

Vjerujemo da sve kolege sistem-inženjeri znaju što znači podatak "Hits" u mail logovima, koji se nalazi u retcima koje upisuje amavis (za one koji ipak nisu sigurni, to je spam ocjena - *score* - koji je tom mailu dodijelio SpamAssassin). No, na tom mjestu se može naći vrijednost koju ne očekujemo (jer smo stavili nekoga u black listu i slično), ili jednostavno oznaka "-". Što to znači? Je li to ocjena "0.0"?

Ukratko, odgovor je "ne". Kad na mjestu ocjene stoji samo crtica (ili minus, kako vam je lakše), to znači da se provjera maila SpamAssassinom **nije uopće obavila**. Postoji nekoliko razloga zašto.

Prvi razlog je taj što je SpamAssassin provjera dosta kompleksna i samim tim traje neko vrijeme, što može značiti znatno opterećenje sustava u slučaju većeg mail prometa. Iz tog razloga, autor Amavisa je ugradio zaštitnu mjeru, pa se ne pregledavaju mailovi veći od 200 kilobajta (spamovi su obično puno kraći od tog). Dakle, svi mailovi veći od 200 kiB neće biti pregledani, **pa čak i ako ste neku adresu stavili u black listu**.

Varijabla koja kontrolira ovu vrijednost se nalazi u datoteci **/etc/amavis/conf.d/20-debian_defaults**:

```
$sa_mail_body_size_limit = 200*1024;
```

Drugi razlog može biti da ste određene primatelje stavili u popis onih koji bezuvjetno primaju poštu. Ove primatelje možete definirati preko nekih od mapa iz skupine **@bypass_spam_checks_maps**, uz istovremeno podešavanje varijabli iz skupine **@spam_lovers_maps**. Više o podešavanju možete naći u dokumentaciji, ili na adresi http://www200.pair.com/mecham/spam/bypassing.html [1].

Treći razlog je jednostavno nekakva greška, ili *timeout* spamassassina. Ove ćete probleme lako uočiti, jer će svi mailovi biti neocjenjeni, ili se uopće neće isporučiti. Uglavnom, brzo ćete vidjeti da nešto "ne štima".

Zašto je uopće nekome bitno da su svi mailovi ocjenjeni? Prikazat ćemo to na primjeru iz prakse, kada se kolega požalio da mu korisnici ipak ponekad dobiju mail s adrese koju je davno blokirao:

```
Mar 27 21:36:32 server1 amavis[29875]: (29875-01) Blocked
SPAM, [IP1] [IP2] <korisnik@domena.hr> -> <user@local.hr>,
quarantine: 9/spam-9fHcA9EbdKvM.gz, Message-ID:
<01a701cacded$28826d60$79874820$@korisnik@domena.hr>,
mail_id: 9fHcA9EbdKvM, Hits: 98.229, size: 27742, 5644 ms

Mar 27 21:43:34 server1 amavis[30727]: (30727-01) Passed
CLEAN, [IP1] [IP2] <korisnik@domena.hr> -> <user@local.hr>,
Message-ID:
<01c401cacdee$196a2e20$4c3e8a60$@korisnik@domena.hr>,
mail_id: I6pZUFWkgKWs, Hits: -, size: 923456, queued_as:
3A5ED160376, 3067 ms
```

Sistem-inženjer je dodao mail adresu "korisnik@domena.hr" u black listu, u nadi da će spriječiti tu adresu da šalje spam mailove svojim korisnicima:

```
# cat /etc/spamassassin/local.cf
blacklist_from korisnik@domena.hr
```

No, iako je u prvom pokušaju mail blokiran, u drugom je propušten bez provjere. Sada kada znamo sve gore navedene činjenice lako je uočiti da je drugi mail daleko veći, svakako veći od navedenih 200 kiB, te je iz tog razloga jednostavno propušten. Lako je izračunati da bi pregledavanje 900 kiB drugog maila trajalo jako dugo, ako je prvi mail od 27 kiB pregledavan preko 5 sekundi.

Što učiniti da ipak blokiramo određene adrese? Najbolje bi bilo uopće ne blokirati pojedine adrese, nego ovakve slučajeve prijavljivati nadređenom ISP-u na adresu koju rabi abuse služba (npr. abuse@carnet.hr ukoliko je korisnik poslao mail iz CARNet mreže).

Ukoliko ipak želite blokirati adrese preko black lista, možete ih napraviti direktno u amavisu, ali i "ispred", u Postfixu. Ovo možete postići preko parametra smtpd_sender_restrictions.

Dakle, imamo čak tri mjesta gdje možemo postići blokiranje određenih adresa (ili domena), a svako mjesto ima određene prednosti i mane. Možda je najbolje ne rabiti sva tri sustava istovremeno, jer ćete se teže snaći i pronaći problem ukoliko se pojavi. No, to ostavljamo vama da odlučite.

- Logirajte [2] se za dodavanje komentara

sri, 2010-03-31 11:57 - Željko Borš**Kuharice:** Linux [3]
Kategorije: Servisi [4]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/734

Links
[1] http://www200.pair.com/mecham/spam/bypassing.html
[2] https://sysportal.carnet.hr/sysportallogin
[3] https://sysportal.carnet.hr/taxonomy/term/17
[4] https://sysportal.carnet.hr/taxonomy/term/28