SpamAssassin: bijele liste (whitelist)

Iako efikasna, zaštita od neželjene pošte (*spama*) nikada neće biti savršena. S kombiniranjem više sustava zaštite, kako je to napravljeno u standardnim CARNetovim konfiguracijama, postotak zaustavljene nepoželjne pošte se znatno podiže. Ipak, uvijek ostaje određeni postotak *false-negativa*, odnosno poruka koju nisu označene kao spam. Slično tome, javlja se i druga situacija: *false-positive*. *False-positive* je poruka **pogrešno** označena kao spam. Kao takva, višestruko je štetnija nego false-negative, jer ta poruka je bila namjenjena upravo vama, pa tako može doći do nepotrebnih neugodnosti.

Zašto do lažnih pozitiva uopće dolazi? SpamAssassin svaku poruku pregleda, i na osnovu pravila koje dolaze s njim (ali i dodatnih, npr. SARE) određuje vjerojatnost da je određena poruka spam. Pravila donose određene bodove (*score*), te ako ti bodovi prelaze određenu razinu (obično oko 5 ili 6), e-mail poruka se označava kao spam.

Problem nastaje jer određene karakteristike dijele i legitimni mailovi i spam. Ukoliko se skupi dovoljno bodova, poruka će biti stavljena u karantenu. Pri tome primatelj ne dobija nikakvu obavijest o tome (jer kad bi dobijao, u njegovom pretincu bi se nalazio jednak broj obavijesti da su spamovi prema njemu zaustavljeni, baš kao da su ti isti spamovi jednostavno propušteni prema njemu).

Objasnit ćemo kako kroz SpamAssassin propustiti određene adrese, bilo da se adrese odnose na primatelja, bilo na pošiljatelja.

Bijele liste

Antispam sustav u CARNetovim paketima je podešen tako da se cijela analiza radi preko jednog korisnika, pod kojim se vrti cijeli sustav antivirusne i antispam zaštite, a obično je to korisnik "amavis". Konfiguracija se nalazi u datoteci /var/lib/amavis/.spamassassin/user_prefs, a izdvojit ćemo najzanimljiviji dio:

```
whitelist_from          LISTSERV.NTBUGTRAQ.COM
whitelist_from          MAILER-DAEMON
whitelist_from          ossecm@localhost.domena.hr
whitelist_from          root@domena.hr
whitelist_from_rcvd     *@net.hr        iskon.hr
whitelist_from_rcvd     *@iskon.hr      iskon.hr
whitelist_to            pero@domena.hr
more_spam_to            pero@domena.hr
all_spam_to             root@domena.hr
```

Kao što se može vidjeti, određenim adresama je preko direktive "whitelist_from" umjetno smanjen spam score. Spam score se izračunava preko internih (Bayes), ali i vanjskih postupaka (DCC, Razor). Osnovna vrijednost je 5.0, što znači da se svaki mail ispod tog iznosa ne smatra spamom, a iznad je, naravno, obrnuto. U CARNetovim paketu amavisd-cn se rabe i više vrijednosti kako bi se izbjegli "lažni pozitivi", odnosno mailovi koji su pogrešno identificirani kao spam.

Whitelist_from će spam score smanjiti za 6 bodova, i omogućiti da manji broj mailova od tog korisnika bude označen kao spam.

No, kako je moguće u svakom e-mail klijentu postaviti lažnu odlaznu adresu, tako je i

"whitelist_from" direktiva podložna ovoj prijevari. Zbog toga postoji i "jača" inačica ove direktive, "whitelist_from_rcvd". Uporaba ove direktive znači da se osim u From zaglavlje maila, gleda i Received zaglavlje, što znači da prijevare više nisu tako lako moguće. Dodatno, ovime je omogućeno da pojedini ISP-ovi bez problema šalju mailove s drugačijim odlaznim domenama, kao što u primjeru stoji da Iskonovi poslužitelji mogu slati mailove s "net.hr" odlaznom domenom. Ukoliko rabite ovu direktivu, na prvo mjesto odlaze domene, a na drugo mjesto dolazi konkretni poslužitelji s kojih mailovi stižu.

Ako smanjenje od 6 bodova nije dovoljno, postoje i druge direktive. Ukoliko se određeni korisnici žale da ne dobijaju neke e-mailove (iako su provjereno) poslani, iskoristite direktivu "**more_spam_to**":

```
more_spam_to pero@domena.hr
```

Direktiva "more_spam_to" će smanjiti *score* za **20 bodova**, što će sasvim sigurno onemogućiti da bilo koji "legalni" mail bude označen kao spam. Za određene situacije preostaje još i direktiva "**all_spam_to**":

```
all_spam_to root@domena.hr
```

Direktiva "all_spam_to" smanjuje score za čak **100 bodova**, što znači da će root korisnik primiti sve poruke koje su mu poslane, uključujući i spam. Ne postoje direktive "more_spam_from" i "all_spam_from" - umjesto toga rabite "whitelist_from" i "whitelist_from_rcvd".

Također, možete generirati listu adresa za bijelu listu iz vašeg lokalnog LDAP poslužitelja. U cron postavite (sve je u jednoj liniji):

```
0 * * * * ldapsearch -x -b 'dc=domena,dc=hr' | grep mail | awk '/^mail:/
  {print "whitelist_from " $2}' > /var/lib/amavis/.spamassassin/whitelist_from_ldap.t
xt
```

U user_prefs datoteci samo uključite ovu datoteku pomoću direktive "include":

```
include whitelist_from_ldap.txt
```

Za ovim receptom, uglavnom, nema potrebe, ali je dobro znati da se i to može.

Ovo je samo dio mogućnosti SpamAssassina u radu s bijelim listama, pa provjerite dokumentaciju na adresi http://spamassassin.apache.org [1] ukoliko želite saznati više. Drugi puta ćemo malo pojasniti rad s automatskim bijelim listama (AWL) i, naravno, crnim listama.

- Logirajte [2] se za dodavanje komentara

pon, 2009-01-26 15:19 - Željko Boroš**Kuharice:** Linux [3]
Kategorije: Servisi [4]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/483

Links
[1] http://spamassassin.apache.org
[2] https://sysportal.carnet.hr/sysportallogin
[3] https://sysportal.carnet.hr/taxonomy/term/17
[4] https://sysportal.carnet.hr/taxonomy/term/28