SpamAssassin: automatske bijele liste (AWL)


Kako smo prije nekoliko dana i obećali, opisat ćemo SpamAssassinov mehanizam automatskih bijelih lista, Auto-whitelist (AWL). Sam naziv je zapravo pogrešan, jer mehanizam AWL može djelovati i kao crna lista, a objasnit ćemo zašto do toga može doći.

AWL je zapravo metoda dodjeljivanja novog scorea mailovima na osnovu prijašnjih ocjena (*score averaging*), odnosno, ujednačavanje scorea po srednjoj vrijednosti prijašnjeg i scorea za e-mail poruku trenutno u obradi. Možda je najbolje to ilustrirati primjerom.

Pretpostavimo da je vaš *cut-off* limit u SpamAssassinu postavljen na 5.0, dakle sve iznad te vrijednosti je spam. Poznanik vam je poslao mail koji je dobio score od ravno 0 bodova. No, za nekoliko dana vam isti poznanik proslijeđuje mail koji ovaj put dobija score od čak 8 bodova, te bi bez AWL-a bio zaustavljen kao spam. AWL u ovoj situaciji izračunava novi score, koji sad iznosi 4 boda, i mail može proći do primatelja. Sljedeći mail od istog pošiljatelja će biti ujednačen sa ovom, novom, vrijednošću. Na ovaj način, AWL ujednačava scoreove i briše ekstremne vrijednosti (*peakove*), što je na određeni način "poštenije" jer daje priliku određenim pošiljateljima da njihovi mailovi ipak kasnije prolaze. Ako takvi pošiljatelji nastave slati mailove koji dobijaju visok score, ni AWL im više neće pomoći da ostanu ispod praga od 5.0 bodova.

Zašto smo spominjali AWL u pomalo negativnom kontekstu, da može djelovati i kao crna lista? Upravo zbog tog mehanizma ujednačavanja scorea, svaki pošiljatelj koji ima visok score u AWL bazi teško će se "izvući" sa novim mailovima, iako imaju nizak score. Primjerice, neki drugi pošiljatelj je poslao prvi mail sa visokim scoreom od 30 bodova. AWL će svaki njegov novi mail ujednačiti sa prethodnim scoreom, pa ako je njegov novi mail dobio score od 4 boda, AWL će taj score povećati na čak 17 bodova, jer je srednja vrijednost (30 + 4) / 2 = 17. Iako bi pošiljateljev mail bez AWL prošao, nakon AWL-a će biti zaustavljen. Bit će potrebno još nekoliko mailova s izrazito niskim scoreom da bi taj pošiljatelj bio oslobođen iz AWL "kaveza".

Naravno, u slučaju da postoji potreba, tog korisnika možete ručno izbaciti iz AWL baze:

```
# su -c "spamassassin --remove-addr-from-whitelist korisnik@domena.hr"
```

Naredbu "su" rabimo jer se provjera spama na CN-Debian sustavima radi preko korisnika "amavis", pa je stoga potrebno maknuti tu adresu iz baze baš tog korisnika.

Možemo provjeriti je li korisnik obrisan iz baze:

```
# su -c "check_whitelist | grep korisnik@domena.hr"
```

Ispis skripte check_whitelist prikazuje tri informacije, trenutni score određenog korisnika, te u zagradi ukupni score i broj poruka s te adrese):

```
# su -c "check_whitelist" amavis  | sort -n
    -7.0       (-14.1/2)  --  confirmation@pay-pro.com|ip=88.81
    -5.9     (-351.9/60)  --  logcheck@domena.hr|ip=none
    -5.9   (-1076.0/183)  --  sophos@domena.hr|ip=161.53
    -5.9   (-2428.8/413)  --  virusupdates@domena.hr|ip=none
```

```
    -5.4      (-91.7/17)  --  korisnik@domena.hr|ip=none
...
```

Inače, sa skriptom check_whitelist se po kriteriju broja pojavljivanja mogu masovno brisati nepotrebni zapisi, jer se provjera spama zbog dugogodišnje AWL baze (preko sto megabajta ili više) zna bitno usporiti ili čak potpuno zablokirati. Iz tog razloga AWL baza se u CARNet paketu spamassassin-cn preko cron datoteke /etc/cron.monthly/spamassassin-cn smanjuje jednom mjesečno, brišući sve unose koji se pojavljuju samo jednom.

Skripta dolazi zajedno s paketom spamassassin-cn, i prima samo tri parametra:

```
# check_whitelist [--clean] [--min n] [dbfile]
```

Bez parametra "--clean" samo će se ispisati sadržaj baze, a parametar "--min" određuje limit do kojeg će se e-mail adrese brisati (pretpostavljena vrijednost je 2, dakle brisat će se svi mailovi koji se pojavljuju samo jednom u bazi).

AWL baza se na CARNetovim poslužiteljima nalazi u datoteci /var/lib/amavis/.spamassassin/auto-whitelist. Funkcionalnost AWL-a možete ugasiti tako da u datoteku /var/lib/amavis/.spamassasin/user_prefs upišete:

```
use_auto_whitelist 0
```

Naravno, bit će potrebno restartati amavisd-new nakon toga.

Više informacija možete pronaći na adresi http://spamassassin.apache.org [1] i http://wiki.apache.org/spamassassin/ [2].

- Logirajte [3] se za dodavanje komentara

sub, 2009-01-31 11:40 - Željko Borš**Kuharice:** Linux [4]
Kategorije: Servisi [5]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr/node/509

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