SpamAssassin savjeti i trikovi

SpamAssassin je vjerojatno najpoznatiji sustav zaštite od neželjene pošte (*spama*). Na ovim stranicama ćemo pokušati opisati najčešće probleme i najefikasnije načine konfiguracije koje su proizašle iz dugogodišnje uporabe.

- Logirajte [1] se za dodavanje komentara

DCC (Distributed Checksum Clearinghouse) izbačen iz Debianovih repozitorija

DCC (Distributed Checksum Clearinghouse) [2] je popularan servis za filtriranje spam poruka na mail poslužiteljima i kao takav je prisutan već dulje vrijeme u CARNetovoj distribuciji Debiana, uglavnom preko SpamAssassina. No, kako su neki sistem inženjeri mogli primjetiti, odnedavno ovaj paket nije moguće instalirati na poslužitelj na uobičajen način.

Razloga su dva: prvi je postojanje važnog sigurnosnog propusta, kojeg Debian sigurnosni tim nije mogao popraviti zbog prevelikih razlika u inačicama DCC-a u stabilnoj distribuciji Debiana i aktualnog izvornog koda DCC-a. Opcija koja u takvim slučajevima postoji je izvanredno ubacivanje aktualne inačice DCC-a u stabilnu distribuciju Debiana (što se rijetko radi). To nije učinjeno jer je u međuvremenu DCC-ova licenca promijenjena i nije više u skladu s GPL-om kojeg Debian distribucija striktno poštuje.

Iz tih razloga DCC je jednostavno izbačen iz službenih Debian repozitorija. Paketi koji ovise o DCC-u su prilagođeni da više o njemu ne ovise, pa tako i CARNet paket **spamassassin-cn**. Ovaj paket od inačice **2:3.1.7-4** više ne ovisi o DCC-u. Ovo ne znači da i dalje ne možete rabiti DCC, ali ga morate naći na nekom neslužbenom repozitoriju ili paket sami napraviti. Naravno, morate obratiti pažnju na licencu [3] kako je ne biste prekršili.

- Logirajte [1] se za dodavanje komentara

ned, 2008-08-31 19:14 - Željko Boroš**Vijesti:** Linux [4]
Kategorije: Servisi [5]
Vote: 0

No votes yet

story_tag: dcc [6]
spamassassin [7]
rhyolite [8]

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 [9] i http://wiki.apache.org/spamassassin/ [10].

- Logirajte [1] se za dodavanje komentara

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

Vaša ocjena: Nema Average: 5 (1 vote)

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 [9] ukoliko želite saznati više. Drugi puta ćemo malo pojasniti rad s automatskim bijelim listama (AWL) i, naravno, crnim listama.

- Logirajte [1] se za dodavanje komentara

pon, 2009-01-26 15:19 - Željko Borš**Kuharice:** Linux [11]
Kategorije: Servisi [5]
Vote: 0

No votes yet

SpamAssassin: crne liste (blacklist)

Zadnji članak u nizu članaka o SpamAssassinovim bijelim [12], AWL [13] i crnim listama pokriva, naravno, crne liste. Kako spameri kod slanja neželjenog maila često mijenjaju odlaznu adresu (a često i svaki mail ima drugačiju, programski generiranu adresu), njihovo upisivanje u crnu listu često nema smisla. No, u određenim slučajevima crne liste ipak mogu dobro doći, primjerice kod primanja reklamnih mailova od strane nekih domaćih ponuđača, koji najčešće ne mijenjaju adresu. Neki od njih jednostavno ignoriraju sve zamolbe da prestanu slati reklame, pa je najjednostavnije rješenje staviti ih na crnu listu.

Kao i kod bijelih lista, direktive se upisuju u datoteku user_prefs, a sintaksa je jednostavna:

```
blacklist_from      frankcollins74@yahoo.fr marketing@tvrtka.hr
```

Naravno, moguće je rabiti i wildcard znakove:

```
blacklist_from     *@tvrtka.hr
```

Ovime će cijela domena biti stavljena na crnu listu.

Ukoliko se adresa pojavljuje u nekom od polja u zaglavlju To:, Cc:, Resent-To: i slično, možemo upotrijebiti varijaciju direktive blacklist, blacklist_to:

```
blacklist_to      user@domena.hr
```

Upravljanje crnim listama je moguće i preko naredbene linije:

```
su -c "spamassassin --add-addr-to-blacklist=adresa@domena.hr" amavis
```

Nakon izvršavanja ove naredbe, adresa "adresa@domena.hr" će biti dodana u trajnu bazu crnih i bijelih lista. Pa koja je onda razlika između dodavanja adrese u user_prefs datoteku i dodavanja direktno u bazu? Sa stanovišta krajnjeg korisnika, skoro nikakva, ali ih ima. Stavljanje određene adrese u crnu listu dodaje joj score od 100 bodova, podjednako za oba načina.

Prva bitna razlika je u brzini aktivacije, jer dodavanje adrese preko naredbene linije odmah postaje aktivno, dok nakon dodavanja u konfiguracijsku datoteku /var/lib/amavis/.spamassassin/user_prefs treba restartati spamassassin, odnosno u našem slučaju amavis.

Za pošiljatelje s adresa koji dulje vrijeme ne poštivaju zamolbe o skidanju s njihovih reklamnih mailing lista najjednostavnije je trajno ih dodati u user_prefs. Preko naredbene linije je možda najbolje dodavati adrese koje vas trenutno zasipaju neželjenim mailom. No, konačna odluka ovisi o situaciji na poslužitelju i vašoj sigurnosnoj politici. Ne zaboravite da, ukoliko imate aktivan AWL, blacklistana adresa nakon nekog vremena (i nekoliko regularnih mailova s niskom ocjenom) može pasti ispod razine spama! Više o ovoj pojavi pročitajte u članku [13].

Brisanje iz baze (koja se nalazi u datoteci /var/lib/amavis/.spamassassin/auto-whitelist) se radi s opcijom:

```
su -c "spamassassin --remove-addr-from-whitelist=adresa@domena.hr" amavis
```

Moramo napomenuti da ne postoji opcija --remove-addr-from-blacklist, ali kako se ista baza dijeli za sve blacklist, AWL i whitelist unose (samo su dodjeljeni drugi scoreovi), potpuno je svejedno i može se upotrijebiti opcija --remove-addr-from-whitelist.

Kasnije, upoznat ćemo vas sa mogućnostima pravljenja vlastitih pravila unutar SpamAssassina, kako testirati ta pravila i kako održavati SpamAssassin kako bi kroz vrijeme i dalje ostao efikasan.

- Logirajte [1] se za dodavanje komentara

ned, 2009-02-08 17:00 - Željko Borš**Kuharice:** Linux [11]
Kategorije: Servisi [5]
Vote: 0

No votes yet

SpamAssassin: nova inačica 3.2.5

 Kao priprema za nadolazeće Debianovo izdanje Lenny, jedan od tranzicijskih paketa koji ćemo uskoro moći instalirati je i spamassassin-cn. Osim što donosi brojna poboljšanja i ispravke grešaka od inačice 3.1.7, ovo je prva inačica koja u sebi sadrži dodatne zaštite specifične za naše područje. Konkretnije, radi se o nekoliko inačica *phishing* spamova, čak i nekoliko manje ili više uspješno prevedenih na hrvatski jezik, koji u ovih nekoliko zadnjih dana kruže po Hrvatskoj. Zajednička im je činjenica da od korisnika traže slanje e-mail adrese sa odgovarajućom zaporkom, predstavljajući se kao web ili mail administratori.

Kako je CERT [14] zaprimio više ovakvih spamova, odlučeno je da se u novi SpamAssassin ubace i pravila koja će onemogućavati da ovakvi *phishing* spamovi prolaze do korisnika. Ova će se praksa vjerojatno i ustaliti, kako bi zaustavljanje spama bilo brže i efikasnije.

Inačica SpamAssassina 3.2.5 je ujedno i posljednja dostupna inačica u *upstreamu*.

- Logirajte [1] se za dodavanje komentara

pet, 2009-02-13 16:00 - Željko Borš**Vijesti:** Linux [4]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

SpamAssassin: pravila (rules), kako ih promijeniti i kako izbjeći lažne pozitive

 Mogućnost da sasvim legitimni mailovi vaših korisnika budu prepoznati kao spam (*false-positive*) smo već spominjali u člancima u našoj E-knjizi o SpamAssassinu na adresi http://sistemac.carnet.hr/node/486 [15]. Po, u IKT industriji omraženom Murphyjevom zakonu, to će biti upravo mail vašeg pretpostavljenog, ili nekog korisnika koji jednostavno na svaki problem burno reagira i uvijek eskalira problem na više razine.

U redu, našli ste problematični mail i po članku na Portalu "Amavisd-release: oslobodite svoj mail! [16]" vratili mail iz karantene. No, kako sprječiti da se slično više ne ponovi?

Prva stvar je analizirati što je SpamAssassin našao problematično kod specifičnog maila. Ovo nije problem, jer se sve nalazi u SpamAssassin izvješću (ako je tako konfigurirano), ali i u zaglavlju maila u karanteni. Evo primjer iz stvarnog života:

```
X-Spam-Flag: YES
X-Spam-Score: 7.007
X-Spam-Level: *******
X-Spam-Status: Yes, score=7.007 tag=2 tag2=6.31 kill=6.31 tests=[FROM_HAS_ULINE_NUMS=
0.291,
    HTML_30_40=0.374, HTML_MESSAGE=0.001, RAZOR2_CF_RANGE_51_100=0.5,
    RAZOR2_CF_RANGE_E8_51_100=1.5, RAZOR2_CHECK=0.5, UNDISC_RECIPS=0.841, URIBL_BLACK
=3]
```

Sve informacije koje nam trebaju su ovdje. Različite aplikacije rabe različita zaglavlja, a ukratko značenja su:

X-Spam-Flag Mail je spam, jer je prešao određenu razinu (vidi se u zaglavlju)
X-Spam-Score Točna numerička završna razina (score) nakon provođenja svih testova
X-Spam-Level Završna razina zaokružena na cijeli broj, označena brojem zvjezdica
X-Spam-Status Najzanimljiviji redak, koji govori sve što je SpamAssassin zaključio o mailu

U ovom retku možemo vidjeti koja je točna razina spama, koja je razina "rezanja", te razina označavanja (primjerice, želimo vidjeti score maila, iako sam mail neće završiti u karanteni).

U ovom se zaglavlju nalaze svi provedeni testovi, te koju ocjenu su doprinijeli u ukupnom rezultatu. Ova na izgled kriptična imena imaju točno svoja značenja, te se u njihovoj definiciji može vidjeti zašto su se uopće uvažila. Gdje se nalaze te definicije? Većina se nalaziu direktoriju /usr/share/spamasassin, i najbrže ih je naći sa:

```
# cd /usr/share/spamassassin/
# grep -r FROM_HAS_ULINE_NUMS *
20_head_tests.cf:header FROM_HAS_ULINE_NUMS     From =~ /_\S?(?:[a-
```

```
z]+\w*?\d+|\d+\w*?[a-z]+)\w*\@/i
20_head_tests.cf:describe FROM_HAS_ULINE_NUMS   From: contains an underline and numbe
rs/letters
...
50_scores.cf:score FROM_HAS_ULINE_NUMS 0.744 0.217 0.310 0.291
```

Test se sastoji od provjere postoji li u "From" polju, osim slova, i brojevi i podvlaka (_). Zašto je ovo bitno? SpamAssassinova pravila se baziraju na statističkoj analizi milijuna spamova. Kako se u nekom određenom broju spamova pojavljuju baš ovakav oblik, to je označeno kao relevantno i ocjenjeno s koeficijentom statistički određene razine. Konkretno, radi se o imenu "Helena_sofia_dionisio".

NOVO:

Često, problematičnim se mogu pokazati i dodatna SARE pravila, koja se automatski nadograđuju preko cron skripte /etc/cron.daily/spamassasin-cn. Kako se SARE skripte više ne nadograđuju (što znači da je mogućnost preoštre ocjene veća), mnogima će prestanak uporabe SARE pravila biti jedini način da spriječe lažne pozitive. SARE, i drugi dodatni rulesetovi se nalaze u /var/lib/spamassassin/<inačica>, te ih od tamo možete obrisati. Obrišite i cron datoteku.

Kako je dosta teško iz šturog objašnjenja uvijek shvatiti o čemu se radi, najbolje je poslužiti se Googleom. Na taj način ćete, osim detaljnijeg opisa konkretnog pravila, dobiti i načine rješavanja problema s tim pravilom. Naime, nisu sva pravila jednakovrijedna, a i mogu jednostavno biti izbrisana iz distribucije SpamAsassina (npr. ovo se pravilo uopće ne pojavljuje u inačici 3.2.5, ali postoji u inačici 3.1.7).

Pravila se u svakoj novoj inačici SpamAssassina re-evaluiraju, dodaju se nova i nestaju stara. Dakle, Google je u ovim slučajevima "vaš prijatelj". Možda najpoznatije pravilo koje je dosta često znalo praviti probleme je FORGED_MUA_OUTLOOK, koje je označavalo da su zaglavlja krivotvorena tako da podsjećaju na Outlook. Zbog mnogih inačica Outlooka SpamAssassin jednostavno nije prepoznavao zaglavlja i označavao ih krivo kao lažna.

Zbog ovog legitimnog razloga vrijedi smanjiti koeficijente koje ovo pravilo dodjeljuje, ili ga čak u potpunosti anulirati. Jednostavno, u /var/lib/amavis/spamassassin/user_prefs upišite:

```
score FORGED_MUA_OUTLOOK 0
```

i uspješno ste spriječili da Vam ovo pravilo povećava ocjene mailova. Nakon svake promjene unutar SpamAssassina, pogotovo ukoliko mijenjate ili dodajete pravila, poželjno je napraviti provjeru sintaktičke korektnosti:

```
# su amavis -c 'spamassassin --lint'
```

Nikakavih poruka o greškama ne bi trebalo biti, a ukoliko se pojave treba istražiti u čemu je problem i nastajati ga popraviti. O tome, drugi puta.

Na kraju, moramo napomenuti da "petljanje" po SpamAssassinu i mijenjanje pravila napravite samo ukoliko je zaista nužno. Prije toga probajte otkloniti razloge zašto se uopće ta pravila uključuju. Provjerite DNS i reverzni DNS, podesite parametre internal_networks i trusted_networks, zamolite korisnike da ne rabe HTML mail i slično. Nakon pravilnog podešavanja sustava, lažni pozitivi će se događati u puno manjem broju.

- Logirajte [1] se za dodavanje komentara

sub, 2009-03-28 15:25 - Željko Borš**Kategorije:** Software [17]
Spam [18]
Vote: 0

No votes yet

SpamAssassin: zanimljiv slučaj

 Jedan zanimljiv slučaj koji je nedavno došao do nas preko Službe pomoći za sistem-inženjere svakako zaslužuje da ga se zabilježi. Možda će i vama pomoći u rješavanju ovakvih i sličnih problema, jer je upravo nevjerojatno kako se naizgled bezazlene stvari mogu manifestirati na najčudnije načine.

Kolega se požalio da jedan korisnik jednostavno ne može poslati mail. Do prije par dana je "sve bilo u redu". Što je najzanimljivije, korisnikov mail je odbijen na poslužitelju s obrazloženjem da se radi o spamu!

Kako je korisnik slao sasvim legitimne poslovne mailove, ovo svakako nije slučaj nekakvog crva ili otvorenog *relaya*. U zaglavlju maila se, između ostalog, spominjalo i pravilo "FH_HELO_EQ_610HEX". Kao što znate, SpamAsassin radi na način da detektira određene karakteristike svakog maila, te na osnovu tih pravila (*rule*s) dodjeljuje završnu ocjenu (*score*). Ovo pravilo znači da se tijekom SMTP sesije računalo koje šalje mail predstavilo s nizom znakova koji podsjećaju na heksadecimalni kod.

Pokazalo se da SpamAssassin takav način predstavljanja "cijeni" s čak 4 boda, te je, uz zbrajanje drugih ocjena, mail bio zaustavljen. No, zašto se računalo predstavlja s nekakavim heksadecimalnim brojevima, kad je uobičajeno PC-je u DNS-u nazvati "pc-106", "pperic" itd? Kolega sistemac je rekao da je njegov način označavanja PC-a: inicijali korisika plus broj kabineta.

Tako se, između drugih korisnika koji se zovu Tomo, Ružica i slično, pojavio i korisnik Ante Anić iz prostorije 12 na drugom katu. Ime njegovog računala je, prema tome, "aa1202", što je dovoljno da se pokrene SpamAssassin pravilo FH_HELO_EQ_610HEX, koje traži sve znakove duljine od 6 do 10 znakova i koji sadržavaju brojke i slova od A do F. Ili, u *regex* slengu:

```
[A-F0-9]{6,10}
```

Rješenje ovog problema može biti stavljanje korisnika u bijelu listu (po članku http://sistemac.carnet.hr/node/483 [12]), promjena imena računala (čime narušavate vlastitu nomenklaturu) ili smanjivanje ocjene ovom pravilu (po članku http://sistemac.carnet.hr/node/548 [19]). Koji ćete pristup primjeniti, ostaje na vama i konkretnoj situaciji. Svakako je bolje 10 spamova više, nego jedan legitimni mail manje.

Umjesto nekog zaključka, svima je valjda jasno da posao sistem-inžnjera neće nikad biti dosadan, sve dok se ovakvi slučajevi događaju.

- Logirajte [1] se za dodavanje komentara

uto, 2009-03-31 09:54 - Željko Borš**Kuharice:** Linux [11]
Kategorije: Software [17]
Spam [18]
Vote: 0

No votes yet

Spamassassin: blokiranje spama pomoću vlastitih pravila

U službi pomoći za sistemce zaprimili smo nekoliko praktički jednakih upita, a tiču se spama. Naime, u zadnje vrijeme primjećena je pojačana aktivnost spamera, a zajedničko svim tim spamovima je isti sadržaj, dok se adresa pošiljatelja mijenja. Adrese pošiljatelja su redovito one s institucije, mada ima i adresa od starih korisnika kojih više nema na sustavu. Ovo upućuje na to da se spamer, odnosno njegov softver, prilagođava poslužitelju te pokušava prikazati kao da spam potiče s tog poslužitelja. Na taj način pokušavaju zavarati korisnike tako što se čini da mail potiče od njihovih kolega, te su veće šanse da će spam pročitati.

Blokiranje po IP adresama nema smisla, jer se mijenjaju (vrlo vjerojatno se radi o zaraženom relay računalu negdje u svijetu). Kako se Subject poruke ne mijenja (što ne znači da neće!), probajmo eliminirati problem pomoću SpamAssassinove direktoive "header". U datoteku /etc/spamassassin/local.cf upišite:

```
header ESTATE_SPAM              Subject =~ /\bInternational Real Estate Consulting C
ompany needs/
score ESTATE_SPAM               4.0
describe ESTATE_SPAM            Spam sa subjectom: International Real Estate Consult
ing Company...
```

Ne zaboravite restartati amavis nakon ovoga (/etc/init.d/amavis restart). Također, ukoliko imate amavis, ne trebate imati pokrenut proces spamd (osim ako ga rabite u neke svoje svrhe). Amavis ima sve što je potrebno da SpamAssassin radi, kombinacija klijenta (spamc) i SA daemona (spamd) vam ne treba u standardnoj konfiguraciji.

Nego, što smo postigli upisom gornjih redaka? Svakom mailu koji sadrži tekst unutar kosih crta u svom Subjectu će biti povećan spam score za 4.0 bodova. Zašto odmah ne staviti 10, 20 ili više? Ako napravimo tako, Amavis će mail odmah staviti u karantenu, no što ako nam vlastiti korisnici proslijede taj spam mail s upitom što da učine? Mi taj korisnikov mail onda nećemo ni vidjeti, jer će prijeći granicu $sa_kill_level_dflt (koja je po defaultu 5.0 bodova, ali često je podešeno na 6.3 ili 6.9, i to ne treba smanjivati).

Neki kolege prijavljuju da Subject spamova nije uvijek isti, ali da svi imaju istu adresu u tijelu poruke.

SpamAssassin može i tome doskočiti pomoću direktive "body":

```
body SPAM_ADDRESS_1          /\@westeur-consult\.com/
describe SPAM_ADDRESS_1      Spam adresa unutar tijela poruke 1
score SPAM_ADDRESS_1         4.0
```

Dakle, SpamAssassin omogućuje pregled tijela poruka, a sve gore spomenuto vrijedi i dalje, a vrijednost koju ste dodijelili spam scoreu držite nisko kako bi izbjegli lažne pozitive.

- Logirajte [1] se za dodavanje komentara

čet, 2011-03-24 12:43 - Željko Boroš**Kuharice:** Linux [11]
Kategorije: Servisi [5]
Vote: 5

Vaša ocjena: Nema Average: 5 (4 votes)

Spamassassin: nova inačica 3.1.7 donosi neke novosti

Nezamjenljivi i vjerni borac protiv spama, Spamassassin u novom CARNetovom paketu (spamassassin-cn 3.1.7-1) dolazi u novoj major inačici. Ovo sa sobom povlači neke promjene u konfiguriranju, ali i osvježavanju antispam pravila.

Najvažnija promjena u konfiguriranju je uporaba modula. Spamassassinu su njegove pojedine funkcionalnosti odvojene u posebne module, te ih je potrebno eksplicitno uključiti ukoliko ih želite rabiti. Ovo se radi naredbom "loadplugin" u datotekama v3xx.pre (trenutno v310.pre i v312.pre). Ove se datoteke čitaju prije čitanja ostalih konfiguracijskih datoteka (/etc/spamassassin/local.cf i korisničkih local.cf). Tek ukoliko uključite odgovarajući plugin, možete rabiti direktive u local.cf.

Ukliko to ne napravite, ništa se strašno neće dogoditi (osim što, naravno, ta funkcionalnost neće biti dostupna), jedino bi lint mogao izdati upozorenje kod operacije "spamassassin --lint":

```
[12978] warn: config: failed to parse line, skipping: bayes_use_chi2_combining 1
[12978] warn: config: failed to parse line, skipping: dcc_timeout 10
[12978] warn: config: failed to parse line, skipping: dcc_fuz2_max 999999
[12978] warn: config: failed to parse line, skipping: dcc_body_max 999999
[12978] warn: config: failed to parse line, skipping: use_dcc 1
[12978] warn: config: failed to parse line, skipping: dcc_fuz1_max 999999
[12978] warn: config: failed to parse, now a plugin, skipping: ok_languages en hr bs
fi de sl
[12978] warn: lint: 6 issues detected, please rerun with debug enabled for more infor
```

```
mation
```

Konkretno, radi se o tome da je u local.cf ostala direktiva koja uključuje uporabu DCC-a, a da odgovarajući modul nije uključen. Problem, ako ga tako možemo nazvati, se rješava tako da u datoteci /etc/spamassassin/v310.pre otkomentiramo redak

```
loadplugin Mail::SpamAssassin::Plugin::DCC
```

Ovo će riješiti problem koji je nastao jer su u novim inačicama programa, pa tako i u CARNetovom paketu, zbog promjene načina licenciranja DCC i Razor2 moduli zakomentirani. Ovo ne znači da će tako i ostati, i promjena će vjerojatno biti, o čemu ćete biti na vrijeme obaviješteni.

Poruku gdje se spominje "ok_languages" možete izbjeći tako da u istoj datoteci otkomentirate redak:

```
loadplugin Mail::SpamAssassin::Plugin::TextCat
```

Zadnju poruku, "bayes_use_chi2_combining", možete izbjeći (ova opcija je sad uključena po *defaultu i ne treba je posebno uključivati*) tako da u /etc/spamassassin/local.cf zakomentirate redak

```
#bayes_use_chi2_combining 1
```

I na kraju, spomenut ćemo da se za sustav za osvježavanje *rulesetova* (antispam pravila) sada rabe nativni mehanizmi (*channels*), a ne više alat "Rules De Jour". Osvježavanje se vrši iz crona i potpuno transparentno. Da biste u potpunosti prešli na ovaj način osvježavanja pravila, kod osvježavanja paketa odaberite da želite instalirati održavateljevu inačicu konfiguracijskih datoteka, odnosno cron jobova (stisnite Y u oba slučaja).

Time smo zaključili ovaj kratki pregled novosti, i potencijalnih nedoumica, kod uporabe novog Spamassassina.

- Logirajte [1] se za dodavanje komentara

uto, 2007-10-16 15:47 - Željko Borš**Vijesti:** Linux [4]
Kuharice: Za sistemce [20]
Kategorije: Servisi [5]
Vote: 0

No votes yet

Spamassassin: poruka "***WARNING***: spamassassin --lint failed."

Sistem administratore svaki dan u mailu može dočekati poruka od sustava koju prije nisu vidjeli. No, to je sasvim normalna pojava i dio je posla. Tako ste prije nekoliko dana u mailu možda počeli dobivati poruke slijedećeg sadržaja:

```
***WARNING***: spamassassin --lint failed.
Rolling configuration files back, not restarting SpamAssassin.
Rollback command is:  mv -f /etc/spamassassin/99_sare_fraud_post25x.cf
/etc/spamassassin/RulesDuJour/99_sare_fraud_post25x.cf.2; mv -f
/etc/spamassassin/RulesDuJour/99_sare_fraud_post25x.cf.20070618-1040
/etc/spamassassin/99_sare_fraud_post25x.cf;

Lint output: config: SpamAssassin failed to parse line, skipping:
<HTML><HEAD><META HTTP-EQUIV="Refresh" CONTENT="0.1">
config: SpamAssassin failed to parse line, skipping: <META
HTTP-EQUIV="Pragma" CONTENT="no-cache">
```

Razlog ovim porukama je "Rules Du Jour", skripta koji svaki dan skida najnovije nadogradnje Spamassassin pravila ("rulesetova") s web stranica http://www.rulesemporium.com. Kako navedeni site prije nekog vremena nije radio, došlo je do grešaka u datotekama koje više ne sadržavaju pravila za detekciju spama i generiraju navedene greške.

Rješenje problema je vrlo jednostavno, treba napraviti slijedeće (kao root korisnik):

```
# cd /etc/spamassassin
# rm -f ??_sare*cf RulesDuJour/??_sare*cf
# /usr/sbin/rules_du_jour
```

Ovaj postupak će obrisati sve oštećene datoteke i skinuti nove, ispravne.

- Logirajte [1] se za dodavanje komentara

pon, 2007-06-18 11:31 - Željko Boroš**Vijesti:** Linux [4]
Kuharice: Za sistemce [20]
Kategorije: Servisi [5]
Vote: 0

No votes yet

Spamassassin: problem 2010. godine

 Za problem Y2K ste čuli (i preživjeli), za problem 2038. godine možda, ali što je problem 2010. godine? Iako je na sam problem upozoreno još 2008. godine, greška je loše popravljena, pa se, eto, ponovo pojavila 1.1.2010. godine.

Na Portalu smo vas još prije upoznali [15] s načinom na koji SpamAsassin radi, a jedan od njih je dodjela "kaznenih" bodova (*score*) za nepravilnosti u zaglavljima mail poruka koje generiraju spam programi. Prilično visok score od 3.2 donosi pravilo FH_DATE_PAST_20XX [21]. Opis pravila je "The date is grossly in the future".

Dakle, SpamAssassin je zahvaljujući ovom pravilu davao visok score svim porukama koje su (prividno) bile poslane iz budućnosti. Ovo je jako korisno, ali samo ako je trenutna godina 2008. ili čak 2009, no nema smisla ako je datum 1. siječnja 2010. godine, zar ne? Krivac je spomenuto pravilo u datoteci /usr/share/spamassassin/72_active.cf koje glasi:

```
header FH_DATE_PAST_20XX Date =~ /20[1-9][0-9]/ [if-unset: 2006]
```

I bez velikog poznavanja *regex* pravila, vidljivo je da će se pravilo primjeniti za sve godine od 2010 do 2099. Naravno, Debian je 1. siječnja 2010. izdao hitnu zakrpu u vidu novog paketa spamasassin (kako biste dobili novu inačicu spamassassina, nužno je dodati volatile repozitorij [22] u /etc/apt/sources.list), tako da pravilo nakon nadogradnje glasi:

```
header FH_DATE_PAST_20XX Date =~ /20[2-9][0-9]/ [if-unset: 2006]
```

Dakle, sada su sumnjive sve godine od 2020 do 2099. Valjda neće zaboraviti promijeniti pravilo negdje potkraj 2019?

UPDATE: Postoje prijave da se ni nakon nadogradnje pravilo ne postavi na pravu vrijednost. Ukoliko je to slučaj i kod vas, jednostavno ručno promijenite pravilo, bilo u /usr/share/spamassassin/72_active.cf, bilo u /etc/spamassassin/local.cf. Ukoliko je tamo sve u redu, postoji šansa da se pravilo zadržalo preko SARE pravila u datoteci 00_FVGT_File001.cf, pa to i tamo ispravite.

Inače, mogli ste i sami intervenirati tako da ste u /etc/spamassassin/local.cf upisali

```
score FH_DATE_PAST_20XX 0.0
```

i restartali amavisd-new. Ukoliko jeste, **ne zaboravite kasnije ukloniti** ovu "popravku", jer podatak da je mail došao **iz budućnosti** zaista govori da je riječ o nepravilno formiranom mailu, ili češće, spamu.

Dakle, problem je riješen. Ili ipak nije? Što je s karantenom, možda je neki legalni mail od ponoći 1.1.2010. završio u karanteni? Brzo provjerite karantenu:

```
# cd /var/lib/amavis/virusmails
# find . | xargs zgrep FH_DATE_PAST_20XX
./C/spam-CnMv2U52GlhB.gz:      BAYES_99=3.5, DATE_IN_FUTURE_96_XX=1.439, FH_DATE_PAST
```

```
_20XX=3.188,
./H/spam-HY-Q+F36aZAT.gz:      FH_DATE_PAST_20XX=3.188, FORGED_MUA_OUTLOOK=1,
./N/spam-Nh7SlWYqnj74.gz:      FH_DATE_PAST_20XX=3.188,  FORGED_MUA_OUTLOOK=1,
...
```

Ukoliko se ispiše malo poruka, najjednostavnije je ručno pregledati svaku datoteku i osloboditi mail iz karantene. Postupak smo opisali u članku http://sistemac.carnet.hr/node/526 [16].

Ukoliko se pokaže da imate puno takvih mailova u karanteni, možete ih ili sve osloboditi (uz nešto negodovanja korisnika zbog spama), ili dodatno rafinirati pretragu po From: i To: poljima:

```
# find . | xargs zgrep -l FH_DATE_PAST_20XX | xargs zgrep -E '^(From:|To:)'
./w/spam-wZDodfcu7erQ.gz:To: undisclosed-recipients:;
./z/spam-zzQkVZXVgfju.gz:From: Dorothy Smith <dorothyrvilxqmn@hotmail.com>
./z/spam-zzQkVZXVgfju.gz:To: <laura_johnston@praxair.com>
./z/spam-z8Ed41PsTvOy.gz:From: "Lucky Day Lottery"<rubenvanjansen@gmail.com>
...
```

Na ovaj način ćete dobiti (približnu) sliku o kakvim se mailovima radi, i treba li ih osloboditi iz karantene ili ne. U svakom slučaju, nešto ručnog pregledavanja i odlučivanja će morati biti.

UPDATED 2010-01-12

- Logirajte [1] se za dodavanje komentara

pon, 2010-01-04 11:53 - Željko Borš**Vijesti:** Linux [4]
Kategorije: Servisi [5]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr/node/486

Links
[1] https://sysportal.carnet.hr/sysportallogin
[2] https://www.rhyolite.com/dcc/
[3] https://www.rhyolite.com/dcc/LICENSE
[4] https://sysportal.carnet.hr/taxonomy/term/11
[5] https://sysportal.carnet.hr/taxonomy/term/28
[6] https://sysportal.carnet.hr/taxonomy/term/376
[7] https://sysportal.carnet.hr/taxonomy/term/90
[8] https://sysportal.carnet.hr/taxonomy/term/377
[9] http://spamassassin.apache.org
[10] http://wiki.apache.org/spamassassin/
[11] https://sysportal.carnet.hr/taxonomy/term/17
[12] https://sysportal.carnet.hr/node/483
[13] https://sysportal.carnet.hr/node/509

[14] http://www.cert.hr
[15] https://sysportal.carnet.hr/node/486
[16] https://sysportal.carnet.hr/node/526
[17] https://sysportal.carnet.hr/taxonomy/term/25
[18] https://sysportal.carnet.hr/taxonomy/term/34
[19] https://sysportal.carnet.hr/node/548
[20] https://sysportal.carnet.hr/taxonomy/term/22
[21] http://wiki.apache.org/spamassassin/Rules/FH_DATE_PAST_20XX
[22] https://sysportal.carnet.hr/node/52