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 [1] 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 [2]. 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 [3] 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 [4].

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 [5] se za dodavanje komentara

pon, 2010-01-04 11:53 - Željko Borš**Vijesti:** Linux [6]
Kategorije: Servisi [7]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr/node/689

Links
[1] https://sysportal.carnet.hr/node/486
[2] http://wiki.apache.org/spamassassin/Rules/FH_DATE_PAST_20XX
[3] https://sysportal.carnet.hr/node/52
[4] https://sysportal.carnet.hr/node/526
[5] https://sysportal.carnet.hr/sysportallogin
[6] https://sysportal.carnet.hr/taxonomy/term/11
[7] https://sysportal.carnet.hr/taxonomy/term/28