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 [1]), promjena imena računala (čime narušavate vlastitu nomenklaturu) ili smanjivanje ocjene ovom pravilu (po članku http://sistemac.carnet.hr/node/548 [2]). 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 [3] se za dodavanje komentara

uto, 2009-03-31 09:54 - Željko Boroš**Kuharice:** Linux [4]
Kategorije: Software [5]
Spam [6]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/546

Links
[1] https://sysportal.carnet.hr/node/483
[2] https://sysportal.carnet.hr/node/548
[3] https://sysportal.carnet.hr/sysportallogin
[4] https://sysportal.carnet.hr/taxonomy/term/17
[5] https://sysportal.carnet.hr/taxonomy/term/25
[6] https://sysportal.carnet.hr/taxonomy/term/34