Spam kao posljedica phishinga

Alati poput *spamassasina* i *amavisa* automatizirali su borbu protiv spama i bez njih je teško zamisliti uredan poslužitelj elektroničke pošte. Međutim, nikakvi nam alati ne mogu pomoći kad korisnici ignoriraju naša upozorenja i nasjednu na prijevare i *phishing*. Upravo je na taj način netko zlonamjeran ovaj put došao do korisničkih podataka jednog od lokalnih korisnika i u kratko vrijeme putem SMTP-a preko poslužitelja poslao desetke tisuća neželjnih e-mailova.

Prvi znak da nešto nije u redu bila je poruka *Nagiosa* o nedostupnosti SMTP servisa. Kako je neobično da na par minuta "pukne" SMTP, a da ostali servisi rade, krenuo sam u u istraživanje. Bilo je lako pronaći korisnika s početka priče i prva je ideja bila blokiranje tog korisničkog računa. Međutim, to nije imalo efekta, šteta bila počinjena jer je većina mailova već otišla. Čitanje logova otkrilo je da je red čekanja (eng. *mail queue*) prepun tzv. "*deferred*" mailova. Odredišni poslužitelji imaju svoje sustave za borbu protiv spama, pa poslani mailovi nisu isporučeni nego vraćeni, ali ne i potpuno odbačeni. Ti mailovi su u stanju "*deferred*", a nalaze se u */var/spool/postfix/deferred*. Poslužitelj koji šalje mail i primi takav odgovor ponovo će pokušavati poslati iste poruke, što može potrajati i do 5 dana. Kako nisam mogao ništa napraviti u vezi mailova koji su već otišli, preostalo mi je da rasteretim poslužitelj brisanjem odlaznih poruka u "*deferred*" stanju, pa sam se pozabavio redom čekanja. Nakon malo testiranja, naredbom

```
postqueue -p | grep ^[A-Z\|0-9] | awk '{print $7}' | sort | uniq -c | sort -rn | head
```

dobio sam popis "pošiljatelja" koji imaju najveći broj odlaznih poruka (stavljam navodnike jer je riječ o izmišljenim pošiljateljima). Dobio sam slijedeći rezultat:

```
5463  adrian.bayford1@GMAIL.COM
5203  gillanandadrianbayford@lycos.co.uk
1913  MAILER-DAEMON
488  adrian@aol.com
415  suporte.unifesp@unifesp.br
158  gillia_adrian_@aol.com
110  adrian@unist.hr
3  gillian.bayford@yahoo.co.uk
```

Vidimo da su Gilian i Adrian zatrpali *queue* s trinaestak tisuća "*deferred*" mailova.

U gornjoj naredbi p*ostqueue -p* daje popis cijelog reda čekanja. Taj rezultat filtriramo naredbom *grep* tako što izdvajamo retke koje počinju (^) velikim slovom ili (\|) znamenkom. U njima sedmo polje sadrži e-mail adresu pošiljatelja, koju izdvajamo koristeći *awk*. Zatim sortiramo ove rezultate te sa *uniq -c* dobijemo broj ponavljanja, po kojem još jednom sortiramo rezultat. Na kraju sa *head* prikažemo prvih 10 redaka, koji sadrže "najmarljvije" pošiljatelje.

Preostaje izbrisati mailove s gornjim adresama iz reda čekanja. Pri tome je trebalo pripaziti da se ne pobrišu legitimni mailovi, pa sam iskoristio skriptu *delete_from_mailq.pl* kolege Boroša iz jednog od članaka [1] o Postfixu. Brisanje tolikog broja mailova trajalo je 7-8 minuta. Kako sam u međuvremenu promijenio kompromitiranu lozinku naivnom korisniku, ponovno punjenje reda čekanja ovolikim

brojem spam poruka nije bilo moguće.

I ovaj slučaj pokazuje kako edukacija korisnika nikad ne smije prestati, ali bi možda trebalo promisliti i o načinu na koji bi nepažljivi korisnik snosio svoj dio odgovornosti.

uto, 2012-11-20 12:17 - Mirko Lovričević**Vijesti:** Linux [2]
Kategorije: Spam [3]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr./node/1145

Links
[1] https://sysportal.carnet.hr./node/203
[2] https://sysportal.carnet.hr./taxonomy/term/11
[3] https://sysportal.carnet.hr./taxonomy/term/34