Gljivice, gljivice na sve strane!

 "Pomagaj! Server mi je zagušen spamom, reklamiraju uklanjanje nekih gljivica, s više domena, različite IP adrese, ni tekst nije uvijek isti, sve prolazi kroz SpamAssassin. Sve je puno g l j i v i c a !"

Otprilike je tako glasio jutarnji poziv "sistemca u panici (TM)". To je trenutak koji su svi doživjeli, ali ga zapravo ne bi trebali doživjeti - nikad. Dobro, dobro, ponekad se stvari tako poslože da se ne može biti na više strana odjednom, pa može nastupiti panika. Jedino rješenje je - vježba i priprema za takve situacije.

"Kad bi imali dovoljno vremena, napravili bi bolju pripremu", čuje se negdje iz zadnjih redova. Da, tako je, ali tako nam je kako nam je, vrijeme se mora pronaći. Pokušajte napraviti scenarije **"ŠTO AKO"**.

"Što ako crkne disk, imam li pričuvni? Memorija, imam li dva dodatna keksa memorije? Ispad mreže od 24 sata, kako će moji korisnici slati i primati mail?" Napravite si barem okviran plan reakcije na (ne)predviđene situacije. Napišite upute za druge kolege kada jednom nađete dobar recept. i tako pomognite jedni drugima.

Da se vratimo na originalan problem. Spam. Spameri se prilagođavaju i uče. Sad, čini se, imaju kampanje. Udare s istom temom spama (odnosno poslodavcem) na sve načine, pa tako dobijate mail s različitih nepovezanih domena, IP adresa, a i sam tekst spama se mijenja, pa ručno postavljeni filteri ne zaustavljaju sve ključne riječi. Što možemo učiniti, kakve alate imamo na raspolaganju?

1) **postfix**

Postix ima mogućnost blokirati mailove po sadržaju u zaglavljima, ali i tijelu poruke. To ga čini izuzetno jakim oružjem u našem arsenalu. Upute za podešavanje su na adresi:

https://sysportal.carnet.hr/node/1289 [1]

Potrebno je ručno unijeti ključne riječi, odnosno rečenice, da ne biste blokirali legitimne mailove koji sadrže iste riječi (riječ "gljivice" nije problem blokirati na informatičkom fakultetu, ali jest problem na nekakvom odsjeku za biologiju). Dakle, uzmite što više riječi iz rečenice, a ne samo pojedine riječi:

```
header ESTATE_SPAM              Subject =~ /Nekoliko prskanja i nestale su gljivice
noktiju/
score  ESTATE_SPAM        10.0
describe ESTATE_SPAM            Spam sa subjectom: Gljivice
```

Pravila je potrebno nadopunjavati dok ne pokrijemo spamerov fond različitih inačica maila.

2) **iptables**

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

Iptables će svoj posao odraditi, ali ne možete ići blokirati adresu po adresu. Treba blokirati cijeli mrežni range, što je laka odluka ukoliko se radi o zemljama s kojima obično ne komuniciramo mailom. Ovdje je od pomoći alat "whois":

```
$ whois A.B.C.D
...
inetnum:        A.B.C.0 - A.B.C.255
...
route:          A.B.C.0/23
```

Dakle, može se blokirati cijeli range A.B.C.0/23:

```
# iptables -I INPUT 1 -p tcp -s A.B.C.0/23 --dport 25 -j DROP
```

Sve ovako napravljene blokade treba staviti u kategoriju "maknuti poslije par dana". Nema smisla blokirati cijeli range samo zbog jednog napada, jer možemo imati problem s dostavom legitimnog maila. U znanstveno-istraživačkoj zajednici uobičajeno je da ljudi dopisuju s kolegama iz drugih država i drugih kontinenata (a za koje ne biste pomislili da imaju ikakve veze s vašom institucijom), pa to ne smijete zaboraviti. Blokiranje adresa ograničite samo na port 25, jer je to logično u ovom slučaju. Drugi napadi traže druge portove ili potpunu blokadu njihovih adresa.

Ovo je vatrogasna mjera i nije dobro na ovaj način dugoročno rješavati probleme. Nakon nekog vremena resetirajte iptables.

3) **spamassassin**

SpamAssassin statistički analizira mailove i odlučuje što je spam, a što nije. Provjerite da li SA radi i koje scoreove/ocjene daje spamovima, da slučajno nije izgašen ili slično. Ukoliko SpamAssassin dodjeljuje score 0, nešto ne štima, morat ćete provjeriti svoju instalaciju i postavke.

SpamAssassin isto može blokirati mailove direktno po sadržaju ili naslovu, samo to nema smisla rabiti ako već imate podešen postfix koji to isto radi (i to još ranije, prije Amavisa i SpamAssassina). Kako podesiti pravila možete pročitati na linku:

https://sysportal.carnet.hr/node/842 [2]

4) **fail2ban**

Nažalost, fail2ban slabo radi kad, kao ovdje, "napad" dolazi s više IP adresa. On radi tako da uzme adresu iz logova za pojedini servis i onda broji spajanja u jedinici vremena. Nakon što je broj spajanja prešao limit, blokira tu adresu. Ako spamer pošalje samo tri poruke s jedne IP adrese, pa nakon par sati opet tri, fail2ban ga neće nikada blokirati. Intervencije u obliku produžavanja vremenskog okvira se mogu provesti, ali onda možemo slučajno blokirati legitimne mail servere. Ukoliko želite koristiti i fail2ban "for good measure", upute za konfiguraciju su na adresi:

https://sysportal.carnet.hr/node/542 [3]

pet, 2018-01-19 14:49 - Željko Borš**Vote:** 0

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

No votes yet

story_tag: spamassassin [4]
postfix [5]

Source URL: https://sysportal.carnet.hr./node/1791

Links
[1] https://sysportal.carnet.hr/node/1289
[2] https://sysportal.carnet.hr/node/842
[3] https://sysportal.carnet.hr/node/542
[4] https://sysportal.carnet.hr./taxonomy/term/90
[5] https://sysportal.carnet.hr./taxonomy/term/122

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr