Graylisting

Nebeljena pošta, spam, svima nam zadaje glavobolju. Svaka nova tehnika zaštite od spama samo je potuciklus na koji spameri brzo nalaze odgovore. Zamjene slova brojkama, namjerni tipfeleri, reklamni slogan kao slika... sve su to lukavstva za zaobilaženje filtera protiv spamova.

Kako se onda boriti protiv spama?

Spamerima je najvažnija brzina. Što više isporučenih poruka, na što više adresa, u što kraće vrijeme, pa će i zarada biti veća. Svjesni činjenice da ljudi mijenjaju adrese, primjenjuju nove filtere, da njihov adresar svakog trenutka sve manje vrijedi, spameri su neprestano u žurbi. Na tome se može graditi obrana. Spameri ne provjeravaju kod greške, tj. statusni kod koji im poslužitelji primatelja vraćaju. Kod je u pravilu pozitivan, tj. signalizira da je poruka prihvaćena i proslijeđena. No, u pojedinim situacijama poslužitelj nije spreman za prihvaćanje maila, što daje do znanja kodovima 4xx. Ovi kodovi poručuju pošiljatelju da dostavu pokušaju kasnije. Potpunu listu SMTP kodova možete naći u ovom članku **[1]**.

Kad jednom "ispucaju" sve adrese s valle domene (a to je događaj koji se mjeri sekundama, eventualno minutama), spameri ne pokušavaju ponovno, ili do novoga pokušaja protječe nekoliko sati ili dana. Upravo se na tome temelji novi način obrane od spama - graylisting.

Graylisting

Što su crne i bijele liste može se zaključiti iz samog imena. Siva lista (graylist), služi za privremenu "karantenu" IP adresa koje pokušavaju isporučiti e-pošitu našem poslužitelju. U prvom razdoblju sva se pošta s te adrese odbija. Karantena traje kratko, 15 ili 25 minuta, a nakon toga se IP adresa prebacuje u bijelu listu i pošta se s nje prima određeno vrijeme, najčešće jedan dan.

Za razliku od spamerskog softvera, regularni poslužitelji su podešeni tako da se netsporučena pošta šalje ponovo dok ne nastupi definirani timeout (uobičajeno 3-5 dana). Razmak između pokušaja je najčešće petnaestak minuta.

Ova jednostavna razlika u načinu rada bit je ideje obrane putem graylistinga. Svaki regularni mail ("ham") nakon nekoliko pokušaja bit će uspješno isporučen, a nakon toga svaki sljedeći s te adrese neće se zadržavati. Kako spameri ne provjeravaju uspješnost isporuke, neće ni znati je li poruka isporučena, a njihov će softver krenuti na drugi niz adresa.

Mane i prednosti

Graylisting nije savršen. Glavna mu je mana očigledna, svaka će se poruka u početku odbiti, što može zasmetati u slučajevima kad je nužna hitnost isporuke. Problem ublažava pažljivo složena inicijalna bijela lista. Dodatna je nevolja što odbijajući poruke opterećujemo udaljene poslužitelje, što će eskalirati kad se mnogi počnu braniti graylistingom.

Druga mana je što spam ipak može proći zaštitu jer je istekao period karantene, a adresa spamera je završila na bijeloj listi. No bijela lista vrijedi samo 24 sata (ili koliko ste već odredili), pa jedan te isti spamer neće moći dugotrajno isporučivati nebeljenu poštu. Također, moguće je njegovu IP adresu staviti u access listu sendmaila i trajno riješiti problem upornih spamera.

Treći i najveći problem je u tome što će se spameri neminovno prilagoditi novom sustavu zaštite. Spamerski softver samo treba malo dograditi, definirati da se svaki odbačeni mail kod kojega grešku nije fatalna pokuša ponovno isporučiti. To bi srušilo temelj ovog sustava obrane, te će on u tom slučaju brzo zastarjeti.

Pozitivne strane primjene graylistinga ne treba više posebno isticati. Koliki će biti dobici ovisi o svakom poslužitelju pojedinačno, njegovoj konfiguraciji te prometu. No, može se reći da graylisting propusnost spama smanjuje od 60 do 80 posto, pa i bolje. Ako se pri tome rabe i klasični filtri (SpamAssassin, razor, pyzor, PureMessage itd.), postotak zaustavljanja spama može prijeći 95%, što će korisnici svakako zamijetiti i znati cijeniti. Trenutačno nema razloga da ne primijenite ovaj sustav, jer nakon primjene nema potrebe za daljim administriranjem, a instalacija je izuzetno jednostavna.

Instalacija

Graylisting se može primijeniti na svakom mail poslužitelju, no ovdje ćemo se ograničiti na CARNetov standard, sendmail. Iskoristit ćemo moćan filter ugrađen u sendmail, milter.

Milter koji ćemo rabiti "inventivno" se zove graymilter. Instalacija je jednostavna. Opisat ćemo

postupak instalacije iz izvornog koda, koji se nalazi na adresi http://www.acme.com/software/graymilter/ **[2]**. Paketa za Debianovu distribuciju trenutačno nema, ali je dostupan paket postgrey za Postfix.

Postupak kompiliranja je standardan i jednostavan:

```
./configure & make & make install
```

Konfiguracija

Najprije treba sastaviti početnu bijelu listu. Kolegijalno upućujemo sve javne operatere u Hrvatskoj, što će spriječiti nepotrebno zadržavanje pošte. U najmanju ruku u datoteku je potrebno staviti CARNet. Unosi u datoteci su rasponi IP adresa (u CIDR notaciji):

```
161.53.0.0/16 # CARNet

193.198.0.0/16 # CARNet

195.29.150.0/8 # T-com

213.191.142.0/8 # Iskon

213.191.133.0/8 # Iskon

83.139.64.5 # X-net

83.139.64.12 # X-net

212.91.96.0/8 # Vipnet

212.91.97.0/8 # Vipnet

213.149.32.0/8 # Globalnet

217.14.208.0/8 # Vodatel

195.78.32.0/8 # Posluh
```

Navedeni su rasponi adresa naših ISP-ova, no popis nije potpun i valja ga prilagoditi lokalnim uvjetima i potrebama. Napomenut ćemo da je u bijelu listu dovoljno staviti samo onaj segment mreže gdje je Mail Exchanger (MX) poslužitelj, a ne cijeli IP raspon određenog ISP-a. Još je bolje staviti samo IP adresu MX poslužitelja, što je poželjno kod kabelskih i DSL operatera gdje su korisnička računala često zaražena virusima i spywareom.

Datoteku s bijelom listom možete nazvati bilo kako, recimo "graymilter_initial_whitelist" i postaviti je u /etc/mail. Naziv i mjesto datoteke podešavaa se u startup skripti.

Parametri

Izvršna datoteka graymilter prima nekoliko opcija:

-graytime seconds

Opcija određuje koliko će dugo IP adresa biti u karanteni, a default je 25 minuta (1500 sekundi)

-whitetime

Ovime se određuje vrijeme u kojemu je IP adresa označena kao sigurna, odnosno svaki mail s ove adrese neće biti zaustavljan u tom periodu.

-initialwhitelist file

Lokacija početne bijele liste. Popunite je uz pomoć uputa iz ovoga članka.

-user user

Korisnik pod čijom se prijavom vrti proces graymiltera. Ovo nije kritično; dovoljno je da je sendmailu dopuštenо čitati početni graymilterov bijeli popis i njegov socket. U obzir dolaze korisnici smmsp, virusen/sweep, a na distribuciji Sarge najvjerojatniji je korisnik amavis.

-nodaemon|-X

Ova opcija određuje da se graymilter neće pokrenuti kao daemon, što može poslužiti kod debugiranja.

-socket

Putanja do graymilter socketa. Preporučamo /var/run/graymilter/graymilter.sock (ili neki kraći oblik).

Startup skripta

Isporučena startup skripta nije pogodna za operativne sustave Debian i Solaris, pa možemo prilagoditi amavisovu startup skriptu:

```
#!/bin/sh

# /etc/init.d/graymilter - start and stop the graymilter daemon

# Zeljko Boros <zelja@ravnica.ptfos.hr> Sun, 10 Apr 2005 20:07:32 +0200

set -e

if [ `uname -s` = "SunOS" ] ; then

PATH=/usr/bin:/sbin:/usr/sbin:/usr/ccs/bin:/usr/local/bin:/usr/local/sbin

MILTER=/usr/local/sbin/graymilter

else

PATH=/bin:/usr/bin:/sbin:/usr/sbin

MILTER=/usr/sbin/graymilter

fi

RUNDIR=/var/run/graymilter

MSOCK=$RUNDIR/graymilter.sock

WHITELIST=/etc/mail/graymilter_initial_whitelist

# Time in seconds (default 25 mins and 2 days, here 15 mins and 2 days)
```

```
GRAYTIME=900

WHITETIME=172800

USER=viruser

test -x $MILTER || (echo "CN: $MILTER is missing"; exit 2)

killkillkill() {

# time to kill

if [ `uname -s` = "SunOS" ] ; then

pkill -f $MILTER >/dev/null 2>&1 || true

else

pkill -u $USER $MILTER >/dev/null 2>&1 || true

fi

sleep 1

rm -fr $RUNDIR

}

case $1 in

start)

killkillkill

if [ ! -d $RUNDIR ] ; then

mkdir -p $RUNDIR

chown $USER:$USER $RUNDIR

chmod 700 $RUNDIR

fi

$MILTER -graytime $GRAYTIME -whitetime $WHITETIME -initialwhitelist \

$WHITELIST -user $USER $MSOCK

if [ $? -ne 0 ] ; then

echo "CN: graymilter start failed! Look at logs for details."

exit 4

fi

sleep 1

;;
```

```
stop)

killkillkill

;;

restart)

killkillkill

exec $0 start

;;

*)

echo "Usage: `basename $0` {start|stop|restart}" >&2

exit 1

;;

esac

exit 0
```

Konfiguracija sendmaila

Ostaje sustav povezati sa sendmailom. To je jednostavna operacija. Upišite sljedeći redak u sendmail.mc:

```
INPUT_MAIL_FILTER(`graymilter', `S=local:/var/run/graymilter/graymilter.sock,

T=S:4m;R:4m')
```

Pokrenite "make -C /etc/mail" ako rabite Linux, a na Solarisu je potreban nešto složeniji naredbeni redak

```
m4 -D_CF_DIR_=/usr/share/sendmail/sendmail.cf /usr/share/sendmail/sendmail.cf/m4/cf.m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
```

Provjera logova

Nakon uspješnog instaliranja, podešavanja i pokretanja, u log datoteci sendmaila bi se trebalo vidjeti zapis poput ovog:

```
Apr 17 10:36:34 ravnica.ptfos.hr graymilter: [ID 175536 mail.info] reading

/etc/mail/graymilter_initial_whitelist
```

Da graymilter radi ispravno vidi se po sljedećim zapisima u mail logu:

```
Apr 17 10:41:40 ravnica.ptfos.hr sendmail[18233]: [ID 801593 mail.info] j3H9fWTC

018233: Milter: from=<saeed_do@in.it>, reject=450 4.7.1 Please try again later.
```

Svaki klijent koji nije u bijeloj listi dobija poruku 4.7.1 Please try again later, a njegova se adresa stavlja na sivi popis. Svake tri minute pregledavaju se IP adrese kojima je istekla karantena, te se one smještaju na bijeli popis.

```
Apr 17 10:44:21 ravnica.ptfos.hr graymilter: [ID 722012 mail.info] graduating 3 addresses to whitelist
```

Poslije toga sve se poruke s te IP adrese primaju bez zadržavanja.

Apr 17 10:50:15 ravnica.ptfos.hr graymilter: [ID 532204 mail.info] 123.456.789.123 is whitelisted ? accepting

Novi sustav za obranu od sveprisutnog spama je spreman za rad. Sretno!

uto, 2005-05-10 16:03 - Željko Borš**Kuharice:** Za sistemce [3]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/101

Links
[1] https://sysportal.carnet.hr/node/106
[2] http://www.acme.com/software/graymilter/
[3] https://sysportal.carnet.hr/taxonomy/term/22