

Graylisting

Nedjeljena pošta, spam, svima nam zadaje glavobolju. Svakla nova tehnika zaštite od spama nam je pokušica na koju spameri brzo nađu odgovore. Zamijene slova brojkama, namjenjeni tipfelovi, nekadni slogan kao vilka... sve su to pokušaji za zaoblazanje filtera protiv spamera.

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 poslužitelj 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 "ispustiš" sve adrese s valja domene (a to je dugotraj) sa mjeti sekundama, eventualno minutama, spameri ne pokušavaju ponovo, ili do nekoga pokušaja prođeće nekoliko sati ili dana. Ispusti se na tome temelji novi način obrane od spama - graylisting.

Graylisting

Što su crni i bijele liste može se sažeti u namotz imena. Svaka lista (graylist), služi za pripremanje "karakteristič" IP adresa koje pokušavaju isporučiti e-poštu našim poslužitelj. U prvom razdoblju sve se pošta s te adrese odbija. Karakteristika 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 radnju od spamerstva softvera, regulirani poslužitelji su podijelili tako da se neregulirana pošta šalje porocno dok ne nastupi defintivni timeout (subotičano 3-5 dana). Razmak između pokušaja je najčešće petnaestak minuta.

Ova jednostavna razlika u načinu rada bit je ključ obrane putem graylistinga. Svakl regulirani mail ("ham") nakon nekakog pokušaja bit će uspjehom isporučen, a nakon toga svaki sljedeti s te adrese neće se zaoblativati. Kako spameri ne prepoznaju uspjehom isporuke, neće ni smati je li poruka isporučen, a njihov će softver trenuti na drugi niz adresa.

Mane i prednosti

Graylisting nije savršen. Glavna mu je mana odgođena, svaka da se poruka u početku odbiti, što može zasmetati u slučajevima kad je nužno hitnost isporuke. Problem ublažava pažljivo skrbena inicijalna bijela lista. Dodatna je nevrijda što odbijaju poruke opterećenjem uslužne poslužitelja, što će eskalirati kad se mnogi poštu brzo zaostaju.

Druga mana je što spam (pak može proći zašto jer je bitan postat karakterima, a adresa spamera je završila na bijeloj listi). Na bijeloj listi vrijedi samo 24 sata (ili koliko ste već odredili), pa jedan te isti spamer može moći dugotrajno isporučivati neželjenu poštu. Također, moguće je ispružiti IP adresu staviti u access listu sendmaila i trajno riješiti problem upornih spamera.

Treći i najgori problem je u tome što da se spameri namotzno prilagubili novom sustavu zaštite. Spameraki softver namo treba malo dograditi, defintivni da se svaki odbaceni mail kad kojega greška nije fatalna poštu ponovo isporučiti. To bi završila baremij ovog sustava obrane, te da on u tom slučaju brzo zaostaje.

Posljednje strane primjene graylistinga ne treba više posebno isticati. Kuliti da bito diktirao u svakom poslužitelju pojedinačno, njegovoj konfiguraciji te prometu. Na, može se reći da graylisting propusnost spama smanjuje od 60 do 90 posto, pa i bodje. Ako se pri tome rabu ključni filteri (Spamassassin, razor, grey, PureMessage itd.), postotak zaustavljanja spama može prijeći 95%, što će korisnici svakako xamijati i smati cijeliti. Translativno nema razloga da ne primijenite ovaj sustav, jer nakon

primjene nema potrebe za daljnjim 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 trenutno nema, ali je dostupan paket postgrey za Postfix.

Postupak kompiliranja je standardan i jednostavan:

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

Konfiguracija

Napomena: Treba sačuvati početnu bazu. Kolegijama upućuje nove javne operatore u Hrvatskoj, što će spriječiti neoprezno zadržavanje pošte. U napravlju radu u datoteku je potrebno staviti CARNET. Uvodi u datoteku su rasponi IP adresa (u CIDR notaciji)

```
161.163.0.0/14 & comment
```

```
189.186.0.0/14 & comment
```

```
195.129.150.0/18 & ?-com
```

```
213.181.142.0/18 & rakus
```

```
219.139.133.0/18 & rakus
```

```
83.139.44.0 & m-net
```

```
83.139.44.12 & m-net
```

```
212.81.98.0/18 & vspnet
```

```
212.81.97.0/18 & vspnet
```

```
213.149.102.0/18 & stobaknet
```

```
217.14.208.0/18 & msk-net
```

```
195.76.32.0/18 & msk-net
```

Navedeni su rasponi adresa malih ISP-ova, no mogu nije potpun i valja ga prilagoditi lokalnim uvjetima i potrebama. Napomenut ćemo da je u bazu listu dovoljno staviti samo onaj segment mreže gdje je Mail Exchanger (MX) poslužitelj, a ne cijeli IP raspon određeni ISP-a. Jaki je bolje staviti samo IP adresu MX poslužitelja, što je poželjno kod kabelekih (DSL) operatera gdje su kontrolna računala često zarađena virusima i spywareom.

Datoteku u bijelom listom možete nazvati bilo kako, recimo "graymilter_mali ISP-ovi" i postaviti je u /etc/mail. Naziv i imena datoteka podjelava se u startup skripti.

Parametri

Uvodi se datoteka graymilter prima redovito opcije:

```
-graytime seconds
```

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

```
-whitelist
```

Opcije se određuje vrijeme u kojemu je IP adresa označena kao sigurna, odnosno kada mail s ove adrese neće biti zadržan u tom periodu.

```
installwhater file
```

Lokacija početne baze liste. Pogonke je sa pomoć uputa iz ovoga članka.

```
-user user
```

Koristi pod tipom sa prijavom vrši proces graymlitea. Ova nije kritična; dovoljno je da je samostalno dopuštene (tjati početni graymlitea bijeli pagla i nigdje nekad. U obzir dolaze koristeći amavis, virusscaning, a na distribuciji Serge najopasniji) je koristeći amavis.

```
-nodaemon 0
```

Ova opcija određuje da se graymlite neka pokrenuti kao daemon, što može poslužiti kod debugiranja.

```
-socket
```

Putanja do graymlite socketa. Preporučamo /var/run/graymlite/graymlite.sock (ili neki drugi abili).

Startup skripta

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

```
#!/bin/sh
```

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

```
# MailDir Mailbox var/lib/daemon/graymlite.dir Mail, 10 Apr 2003 20:07:12 v0.001
```

```
set -e
```

```
if [ "$name" = "start" ] || [ "$name" = "stop" ]
```

```
PATH=/usr/bin:/usr/sbin:/usr/libexec:/usr/bin:/usr/sbin:/usr/libexec:/usr/bin:/usr/sbin
```

```
SCRIPT=/usr/sbin/graymlite
```

```
alias
```

```
PATH=/usr/bin:/usr/sbin:/usr/libexec:/usr/bin:/usr/sbin
```

```
SCRIPT=/usr/sbin/graymlite
```

```
fi
```

```
SCRIPT=/usr/sbin/graymlite
```

```
SCRIPT=/usr/sbin/graymlite
```

```
SCRIPT=/usr/sbin/graymlite
```

```
# End of file /etc/init.d/graymlite
```



```
STARTUP.sh

MYHOSTNAME=localhost

DOMAIN=example

test -e $BUILDDIR || { echo "no $BUILDDIR is existing"; exit 0; }

killallkillall() {

    & time to kill

}

if [ "$name" = "master" ] ; then

    kill -f $BUILDDIR >/dev/null 2>/dev/null || true

else

    kill -u $BUILDDIR >/dev/null 2>/dev/null || true

fi

sleep 1

rm -rf $BUILDDIR

}

case $1 in

start)

killallkillall

if [ -d $BUILDDIR ] ; then

while -p $BUILDDIR

do sleep $BUILDDIR $BUILDDIR

done 100 $BUILDDIR

fi

$BUILDDIR -graylist $BUILDDIR -initiate $BUILDDIR -initialkillall \

$BUILDDIR -copy $BUILDDIR $BUILDDIR

if [ $? -ne 0 ] ; then

echo "no: graylist start failed! look at logs for details."

exit 4

fi

sleep 1

}
```

```
stop

killall kill

:)

sendmail

killall kill

sleep 30 & wait

:)

*)
```

```
echo "usage: 'backdoor 30' (start|stop|restart)" >&2

kill 3

:)

sleep

kill 0

kill 0
```

Konfiguracija sendmaila

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

```
DEFINER_LOCAL_FILTER(`grayfilter', `local/next/nextgrayfiltergrayfilter.aux',

Trif4m,84m)

Pobavite "make -C /etc/mail" ako radite Linux, a na Solarisu je potreban nešto sličniji naredbeni redak

m4 -O _CF_PATH="/usr/share/sendmail/cf" /usr/share/sendmail/cf/m4/m4cf sendmail.mc > /etc/mail/sendmail.cf
```

Prijemna logova

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

```
Apr 17 10:41:38 xenixia.grfon.hr grayfilter: [m 176536 mail.info] sending

/etc/mail/grayfilter_auxial_auxialist

Da grayfilter radi ispravno vidj se po sljedećim zapisima u mail logu:

Apr 17 10:41:48 xenixia.grfon.hr sendmail[14839]: [m 80189 mail.info] 3mefrcr:

01839: Mailer: from=send_mail@.hr, subject=00 4.7.3 Please try again later.

Svakih 5 minuta kopiraju se kopije svih dolaznih poruka 4.7.3. Please try again later, a njegove se adrese stavljaju na svoj popis. Svakih 10 minuta pregledavaju se IP adrese kopirane iz adrese korisnika, te se one upoređuju na bijeli popis.
```

Apr 17 10:41:52 xenixia.grfon.hr grayfilter: [m 112812 mail.info] goodlisting y addressess to whitelists

Posljednja kopija ove se poruke s tog IP adrese primaju bez razdobljenja.

Apr 17 10:50:16 vranica.gpfes.hr graylisting: [pid 632094 maild:1000] 129.456.789.123 is whitelisted & accepting

Novi sustav za obradu od evanprilnog spama je spreman za rad. Sretno!

uto, 2005-05-10 16:03 - Željko Boroš**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>