

Graylisting

Nabrojena pošta, spam, uvijek nam zadaje glavobolju. Svaka nova tehnika zaštite od spama samo je pokušaj na koji spameri brzo nađu odgovore. Zamjene slova brojkama, namjerno ispušteni, reklamni slogan kao vika... sve su to lukavstva za zaobljavanje filtera protiv spamera.

Kako se onda boriti protiv spamera?

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 prosljeđena. 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 "spamer" sve adrese i valde domene (a to je dugačak list) se mjeni sekundama, eventualno minutama, spameri ne pokušavaju ponovo, ili do nekoga pokušaja prođe nekoliko sati ili dana. Ipravno se na tome temelji novi način obrane od spama - graylisting.

Graylisting

Što su crni i bijeli liste može se zaštititi iz samog imena. Svaka lista (graylist), služi za privremenu "kvarantenu" IP adresa koje pokušavaju isporučiti e-poštu našim poslužiteljima. U prvom razdoblju sve se pošta s te adrese odbija. Kvarantena traje kratko, 15 ili 25 minuta, a nakon toga se IP adresa prebacuje u bijelu listu (pošta se s nje prima odredeno vrijeme, najčešće jedan dan).

Za radnju od spamskog softvera, regulirani poslužitelji su podijelili tako da se neopreznost pošta šalje porocno dok ne nastupi defenzivni smisao (subotičano 3-5 dana). Razmak između pokušaja je najčešće petnaestak minuta.

Ova jednostavna zaštita u načinu rada bit je dobra obrana putem graylistinga. Svaki regulirani mail ("ham") nakon nekakvog pokušaja bit će uspjehom isporučen, a nakon toga svaki sljedeći s te adrese neće se zaoblatiti. Kako spameri ne progovravaju uspjehom isporuke, neće ni znati je li poruka isporučena, a njihovu će softver kreirati na drugi list adresa.

Mane i prednosti

Graylisting nije savršen. Glavna mu je mana odgođena, svaka će se poruka u početku odbiti, što može zaostati u slučaju važna kad je nužno hitnost isporuke. Problem ublažava pažljivo sklapanje bijele liste. Dodatna je nevrije što odbijajući poruke opterećujemo uslužbene poslužitelje, što će eskalirati kad se mnogi poštu brzo zaostaju.

Druga mana je što spam (pak može proći zašto) jer je istakao period kvarantena, 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 neće moći dugotrajno isporučivati nabačenu poštu. Također, moguće je naprosu IP adresu staviti u access listu sendmaila i tražiti riješiti problem upornih spamera.

Treći i najopći problem je u tome što će se spameri neminovno prilagoditi novom sustavu zaštite. Spamski softver samo treba malo dograditi, defenzivni da se svaki odbaceni mail šalje kopiju greška nije fatalna poštu ponovo isporučiti. To bi svelo temelj ovog sustava obrane, te će on u tom slučaju brzo zaostati.

Postoje strane primjene graylistinga na treće više posebno bitni: Kako će biti dobri svi u svakom poslužitelju pojedinačno, njegovoj konfiguraciji te prometu. Na, može se reći da graylisting propusnost spama smanjuje od 60 do 80 posto, pa i tođje. Ako se pri tome radi i klasični filter (Spamassassin, razor, pyzor, RspamdMessage itd.), postotak zaustavljenja spama može prijeći 95%, što će korisnici svakako zamijetiti i smati činiti. Tradicionalno nema razloga da ne primjenite 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/graymlter/> **[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 sahatići početnu listu. Količinu upišite kao javne operatore u IPv4skoj, ili sa upisati potrebne zadržavanje podne. U napomenju roku u datoteku je potrebno staviti CARNET. Ovaj u datoteci su rasponi IP adresa (u CIDR notaciji):

161.133.0.0/14 & cernnet

189.148.0.0/14 & cernnet

195.28.150.0/8 & T-com

213.141.142.0/8 & sabnet

219.149.123.0/8 & sabnet

89.139.44.0 & n-gate

89.139.44.12 & n-gate

212.91.98.0/8 & vjsgate

212.91.97.0/8 & vjsgate

213.149.10.0/8 & HSDobri.net

217.14.200.0/8 & msknet.hr

195.76.32.0/8 & hrcn.hr

Napomena: su rasponi adresa malih ISP-ova, no mogu nije potpuni i uvijek su prilagoditi lokalnim uvjetima i potrebama. Napomena: čemo da je u listu listu dodatno staviti samo onaj segment mreže gdje je Mail Exchanger (MX) poslužitelj, a ne cijeli IP raspon određeni ISP-a, jer je bolje staviti samo IP adresu MX poslužitelja, jer je poboljšava kod kabelekih (DSL) operatera gdje su korisnička računala često zaradama virusima i spywareom.

Datoteku u bijelim listom možete nazvati bilo kako, recimo "graymlter_instal_ukoljena" i postaviti je u /etc/mail. Naziv i imena datoteka podjelava se u startup skripti.

Parametri

Datoteka datoteka graymlter prima nekoliko opcija:

graytime seconds

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

ukoljena

Ovime se određuje vrijeme u kojemu je IP adresa označena kao sigurna, odnosno koliko mail u ovoj adresi neće biti paustavljeni u tom periodu.

```
installdeb.sh file
```

Lokacija početne baze liste. Pogonite je uz pomoć uputa iz izvornika.

```
user user
```

Komada kod ovisi se prijavom vrši proces graymlite. Ovo nije kritično; dovoljno je da je samostalno dopuštene (tj. početni graymliteov bazi) pogodi i "argov socket". U obzir dolaze komandi "rmmap", "vncuotestmap", a na distribuciji Sarge najčešćijoj je komand "amavis".

```
daemon0 &
```

Ova opcija određuje da se graymlite neće pokrenuti kao daemon, što može biti korisno kod debugiranja.

```
socket
```

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

```
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
```

```
# 2003-2004 Miroslav Novak [novak@redhat.com] / Red Hat, 10 Apr 2003 20:07:10 +0200
```

```
set -e
```

```
if [ "$name" = "graymlite" ] ; then
```

```
PATH=/usr/sbin:/usr/lib:/usr/bin:/usr/sbin:/usr/local/bin:/usr/sbin:/usr/local/sbin
```

```
HELPER=/usr/sbin/daemon
```

```
else
```

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

```
HELPER=/usr/sbin/graymlite
```

```
fi
```

```
DESCR=/usr/sbin/graymlite
```

```
PROG=/usr/sbin/graymlite.sock
```

```
WRITELOCK=/var/run/graymlite/graymlite.lock
```

```
# This file is licensed under the terms of the GNU General Public License v2.
```

```
DEBUG=on

SMTPD_OPTIONS=

DEFINITIONS=

#add -f DELIVER { [who "not deliver is working" exit 2]

%%!!%!!%!!%

% time to kill

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

%%!! -f DELIVER >/dev/null 2>&1 || true

else

%%!! -f DELIVER >/dev/null 2>&1 || true

fi

sleep 1

# -f DELIVER

}

case $? in

start)

%%!!%!!%!!%

if [ -d DELIVER ] ; then

mkdir -p DELIVER

chmod 700 DELIVER

chmod 700 DELIVER

fi

DELIVER=$(pwd) DELIVER=$(pwd) DELIVER=$(pwd) DELIVER=$(pwd) DELIVER=$(pwd)

DELIVER=$(pwd) DELIVER=$(pwd) DELIVER=$(pwd) DELIVER=$(pwd) DELIVER=$(pwd)

if [ -d DELIVER ] ; then

who "not graylisting start failed look at logs for details."

fi

fi

sleep 1

fi
```


Problemi topa ove se poruke s tih IP adresa primaju bez zadržavanja.

Apr 17 10:50:16 vmail01.carnet.hr: graylisting: [0] 63204 mail.carnet.hr [192.168.1.100] 525 456.769.123 sa: whiteblatad @ acceptmg

Novi sudar sa obranom od neprihvatljivog spama je spreman za rad. Srećno!

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>