

Graylisting

Nedjeljena pošta, spam, svima nam zadaje glavobolju. Svakla nova tehnika zaštite od spama nam je pokušica na koji spameri brzo nađu odgovore. Zamjenjuju slova brojkama, namjenjuju tipfelere, nekadni slogan kao vika... 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 "ispusti" sve adrese s valja domene (a to je dugotrajno) se njeni sekundarni, eventualno mirisni, spameri ne pokušavaju ponovo, ili do nekog pokušaja prođe nekoliko sati ili dana. Ispusti se na tome temelji novi način obrane od spama - graylisting.

Graylisting

Što su crni i bijeli liste može se sažeti u namotaj. Svaka lista (graylist), služi za pripremu "karakterističnog" IP adresa koje pokušavaju isporučiti e-poštu našim poslužiteljima. U prvom razdoblju sve se pošta s te adrese odbija. Karakterna trajanje 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 predviđeni tako da se nespoštuje pošta šalje poruku 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. Svakim regulirani mail ("ham") nakon nekakvog pokušaja bit će uspjehom isporučen, a nakon toga svaki sljedeći s te adrese neće se zaobilažiti. Kako spameri ne prepoznaju uspjehom isporučen, neće ni znati je li poruka isporučena, a njihovi će softveri trenuti na drugu listu adresa.

Mane i prednosti

Graylisting nije savršen. Glavna mu je mana odgođena, svaka da se poruka u početku odbije, što može zasmetati u slučajevima kad je nužno hitno isporučiti. Problem ublažava pažljivo skrbna inicijalna bijela lista. Dodatna je nevrijda što odbijajući poruke opterećujemo uslužne poslužitelje, što će eskalirati kad se mnogi počnu braniti graylistingom.

Druga mana je što spam (pak može proći zašto) jer je bitan period karantina, 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 crnu listu sendmaila i trajno riješiti problem upornih spamera.

Treći i najgori problem je u tome što da se spameri neminovno prilagode novom sustavu zaštite. Spamerški softver samo treba malo dograditi, defintivni da se svaki odbijeni mail kod kojega greška nije fatalna poštu ponovo isporučiti. To bi značilo barem novog sustava obrane, te da on u tom slučaju brzo zaostaje.

Poslovne strane primjene graylistinga ne treba više posebno isticati. Kvaliti da bit diktiraju u svakom poslužitelju pojedinačno, njegovoj konfiguraciji te prometu. Na, može se reći da graylisting propusnost spama smanjuje od 60 do 90 posto, pa i bogđe. Ako se pri tome radi o kvaliteti filtera (Spamassassin, razor, grey, PureMessage itd.), postotak zaustavljanja spama može prijeći 95%, što će korisnici svakako xamijati i znati cijeliti. Translativno nema razloga da ne primijenite svoj 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 kao javne operatore u Hrvatskoj, što će spriječiti neoprezno zadržavanje podne. U napravlju radu u datoteku je potrebno staviti CARNET. Unosi u datoteci su rasponi IP adresa (u CIDR notaciji)

161.123.0.0/16 # CARNET

192.168.0.0/16 # CARNET

195.29.159.0/8 # T-com

213.181.142.0/8 # Iskon

213.181.122.0/8 # Iskon

82.129.64.0 # X-net

82.129.64.12 # X-net

212.81.98.0/8 # Vipnet

212.81.97.0/8 # Vipnet

213.149.102.0/8 # Globalnet

127.0.0.0/8 # Vindax1

195.78.32.0/8 # ProCub

Navedeni su rasponi adresa malih ISP-ova, no popis 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 poželjnije kod kabelekih i DSL operatera gdje su korisnička računala često zarađena virusima i spywareom.

Datoteku u bazi treba čuvati nazivati bilo kako, recimo "graymilter_milna_ukitelu" i postaviti je u /etc/mail. Naziv i mjesto datoteke podebljava se u startup skripti.

Parametri

Uvijek datoteku graymilter prima redovito općenito:

graytime seconds

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

ukitelu

Quine se određuje vrijeme u kojemu je IP adresa označena kao sigurna, odnosno koliko mal i ove adrese neće biti postavljene u tom periodu.



```
GRAYTIME=000

WAITTIME=12000

USER=rootuser

test -s $WGLTR || { echo "Ok: $WGLTR is missing"; exit 2}

killallkillall() {

# time to kill

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

kill -F $WGLTR >/dev/null 2>&1 || true

else

kill -u $USER $WGLTR >/dev/null 2>&1 || true

fi

sleep 1

rm -fr $BUNDLER

}

case $s in

start)

killallkillall

if [ `cat $BUNDLER` ] ; then

mkdir -p $BUNDLER

chmod $USER-$USER $BUNDLER

chmod 700 $BUNDLER

fi

$WGLTR -graytime $GRAYTIME -whitelist $WAITTIME -installwhitelist \

$BUNDLERLIST -user $USER $BUNDLER

if [ $? -ne 0 ] ; then

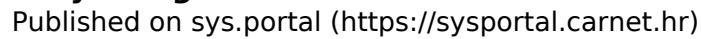
echo "Ok: grayfilter start failed! Look at logs for details."

exit 4

fi

sleep 1

}
```



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

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

Apr 17 18:58:05 remote.ppfes.hr graylistd: [20 522084 mail.info] 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>