AntiSpam

Sunucuda E-Posta Filtreleme

Serdar KÖYLÜ
Gizem Telekomünikasyon Hizmetleri

İstenmeyen Elektronik Postalar mı ?

Bu cevabı bulabilmek sorunun çözümünün en zor kısmıdır

AntiSpam

SPAM Adı Nereden Geliyor ?

Monthy Python - Flying Circus

Bir skeçten alınmadır.

Mücadelenin en zor ve önemli kısmı SPAM olarak kabul ettiklerinizi kesin sınırlarla belirlemektir..

Virüsler, istenmeyen en önemli içerik..

Duyurular.. Alakasız reklam ve propaganda...

Zambia'da 30 Milyon dolarım var !

Sayın Doç. Dr. Mustafa Akgül Hocamız...

SMTP Sunucu.

Internet Bağlantısı
IP Adresi
Bir PC..

E-MAIL Adresleri.

X bin adet e-mail adresi şu fiyata !
Bir kaç yoğun listeye üye olunur.
Bir websuck programı ile web sitelerinden toplanır.
Bir gecede bir virüs yazılır, nete salınır...

Mücadele Yöntemleri ?

SPAM yapan SMTP sunucularını reddetmek..

Kendi SMTP/Proxy sunucularımızdan SPAM'ı engellemek

E-Mail adreslerinin alanen ortada olmasını engellemek

SPAM yapanları BlackHole listlerine bildirmek.

SPAM postaları tespit edip çöpe atmak.

SPAM yapan SMTP sunucularını reddetmek..

SMTP için Authentication işlevi
- POP-Before-SMTP
- SMTP-AUTH

Geçersiz SMTP sunucuların reddi..
- Reverse DNS Kayıtlarının kontrolü
- RBL Kayıtlarının kullanılması
- Pyzor gibi servisler

Kendi SMTP/Proxy sunucularımızdan SPAM'ı engellemek

SMTP-RELAY'ın engellenmesi

- Sadece kendi domain'lerimiz için RELAY izni.

Proxy ve Firewall üzerinden SPAM'ın engellenmesi

- SQUID için CONNECT metodunun reddedilmesi
- SSL Proxy'lerin dikkatli kullanılması.
- SOCKS/WinGate gibi proxy servislerinin dış ağa kapatılması

Mücadele Yöntemleri ?

E-Mail adreslerinin alanen ortada olmasını engellemek

Liste arşivlerinde üye adreslerinin gizlenmesi

groups.yahoo.com

Web sayfalarında e-mail adreslerini karıştırmak

http://search.cpan.org/~miyagawa/Apache-AntiSpam-0.05/

skoylu at gizemcafe dot net
skoylu at gizemcafeNOSPAM dot net
skoylu spamyapma dot net

skNOSPAMoylu at giz-no war-emcafe nokta net

Mücadele Yöntemleri ?

SPAM yapanları BlackHole listlerine bildirmek.

SPAM postaları tespit edip çöpe atmak.

EXE/COM/BAT/PIF ve ZIP (!?) uzantılarını engellemek.

- Ah şu Windows olmasaydı :)
- Makro virüsleri ?

SPAM olma ihtimali yüksek olan mesajları tespit etmek.

- Hangi mesaj nereye kadar SPAM'dır ?
- AI Teknikleri ne kadar güvenilir ?
- Sizce SPAM olan bence hayati önemde olabilir.

REGEXP yöntemi, basit ama çok katı

- kampanya
- free pics
- click

%60 – 70

%40 – 50

AI Teknikleri, olgun değil ama doyurucu

- Histogram yöntemi
- Bayesian Teoremi

%30..95

%25...1

BAYESIAN Teoremi

Thomas BAYES (1702 – 1761) tarafından ortaya konmuş istatistik yaklaşımlar için bir tür öğrenmeye dayalı kestirme yöntemidir.

$$p(H \mid D,I) = p(H \mid I)\frac{p(D \mid H,I)}{p(D \mid I)}$$

$$\frac{(SH)/(TS)}{(SH)/(TS) + (IH)/(TI)}$$

SH: Spam Hits TS: Total Spam Messages
IH: Innocent Hits TI: Total Innocent Messages

EXE/COM/BAT/PIF ve ZIP (!?) uzantılarını engellemek.

```
header_checks =
        regexp:/etc/postfix/maps/header_checks
mime_header_checks =
        regexp:/etc/postfix/maps/mime_header_checks
```

```
/^Subject: .*          / REJECT Too Many Spaces 1
/^Subject: .*f[ _\.\*\-]+r[ _\.\*\-]+e[ _\.\*\-]+e/
     REJECT Hidden 'free' in Subject..
/^Subject: .*free* / REJECT Spam Mail..
```

```
/name=[^>]*\.(bat|com|exe)/ REJECT No Executables
```

SPAM yapan SMTP sunucularını reddetmek..

```
maps_rbl_domains =  relays.ordb.org,
                    inputs.orbz.org
smtpd_recipient_restrictions =
                    reject_unknown_client,
                    permit_mynetworks,
                    reject_maps_rbl,
                    check_relay_domains
smtpd_client_restrictions =
                    reject_unknown_client,
                    reject_maps_rbl
```

Procmail ile pyzor kullanımı

```
:0 Wc
| pyzor check
:0 a
pyzor-caught
```

Çalıştırılabilir dosyaları engelleme

```
:0HB
* ^Content-Type: MULTIPART/MIXED
* ^Content-Disposition: (attachment|inline);
* filename=".*\.(bat|bif|exe|pif|com|vbs)"
        /etc/Procmail/Filtered/virus
```

DSPAM
Statistical Spam Protection

DSPAM, Geliştirilmiş BAYESIAN Algoritması ile son derece başarılı sonuçlar verebilir.

```
mailbox_command =
     /usr/local/bin/dspam -t -Y -a $DOMAIN -d $USER
```

BogoFilter

http://www.paulgraham.com/spam.html
http://www.paulgraham.com/better.html

```
smtp inet n - - - - smtpd

-o content_filter=bogofilter:

bogofilter unix - n n - - pipe \
   user=bfilter \
   argv=/usr/local/sbin/bfilter.sh \
   -f ${sender} -- ${recipient}
```

```
export PATH=$PATH:/usr/sbin
export HOME=/home/filter
cd $HOME
bogofilter -p | sendmail -i "$"
```


SpamAssassin

Http://selwerd.cx/xbl/

Son derece katı kuralları olup en fazla adresi ihtiva etmektedir

http://www.five-ten-sg.com/blackhole.php

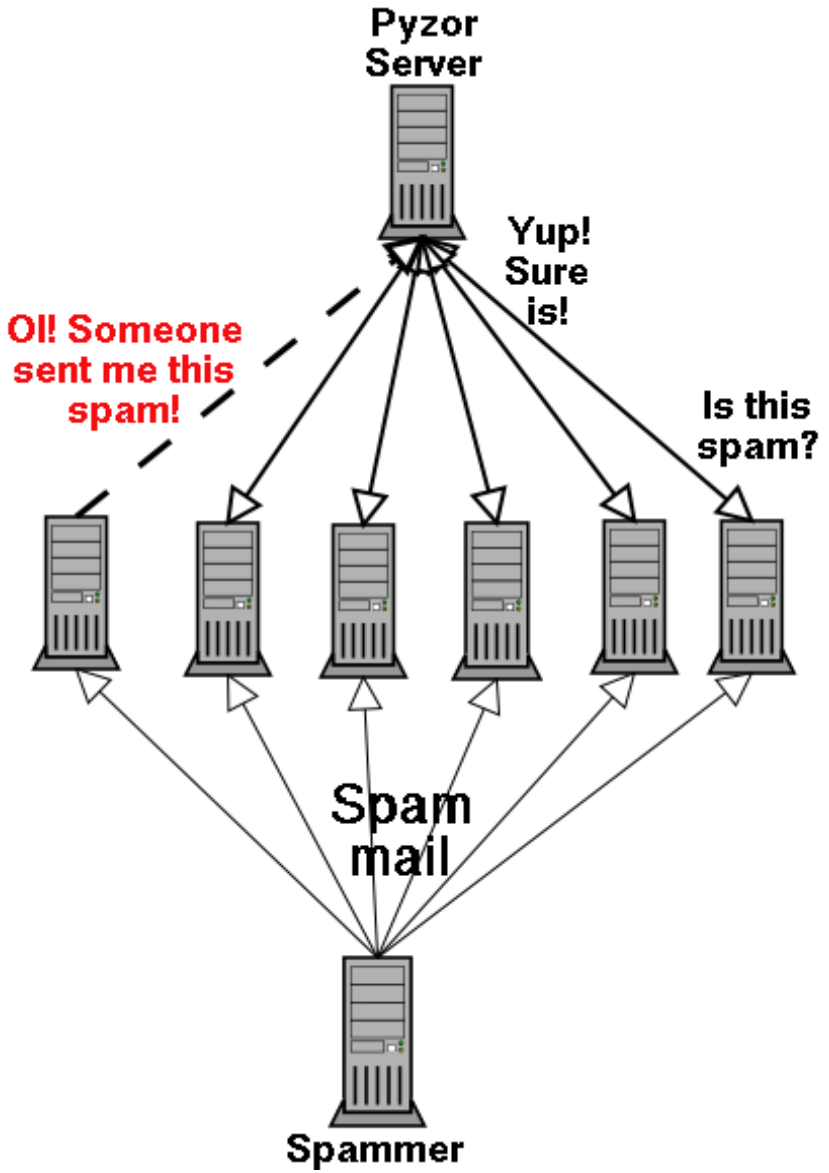
Dialup IP adresleri, free e-mail servisleri vs.

http://www.rfc-ignorant.org/

Genel olarak RFC kaidelerine uymayan servisler..

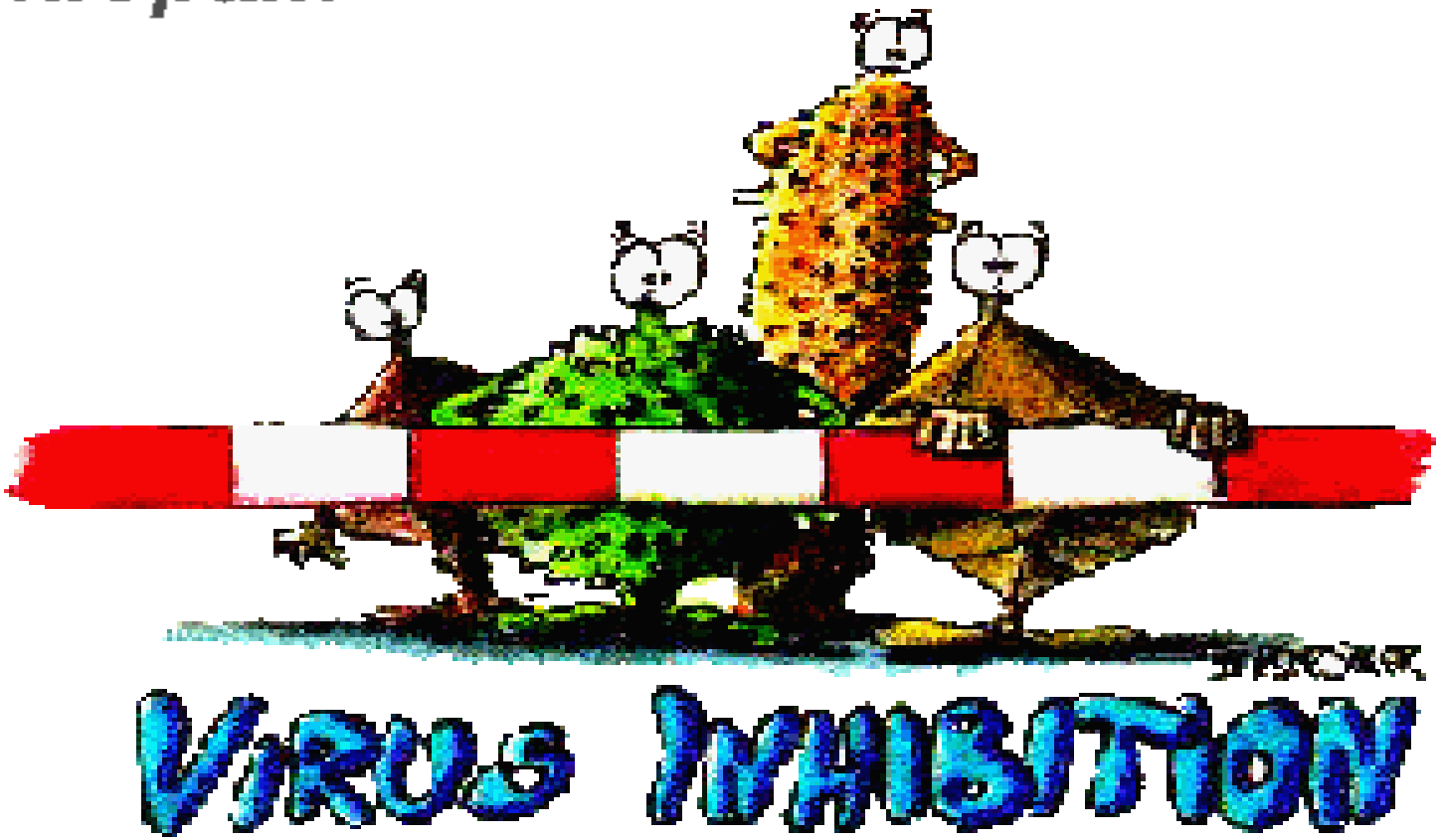
http://www.sdsc.edu/~jeff/spam/cbc.html

RBL servislerinin upuzun ve karşılaştırmalı bir listesi.



SPAM mesajın kullanıcılar tarafından tespit edilerek veritabanına eklenmesi prensibiyle çalışır..

http://pyzor.sourceforge.net


VIRUS INHIBITION