"Oh no, we're being spammed!"

Linux ile SPAM Filtreleme

A. Murat Eren, Çanakkale Onsekiz Mart Üniversitesi, Bilgisayar Mühendisliği Bölümü

```
....
Continuing with this example, you send out only 5,000 e-mails.
With a 0.2% response, that is only 10 orders for report #1.  Those 10
people responded by sending out 5,000 e-mail each for a total of 50,000.  Out
of
those 50,000 e-mails only 0.2% responded with orders.  That's = 100 people
responded and ordered Report #2. Those 100 people mail out 5,000 e-mails each
for a total of 500,000 e-mails.  The 0.2% response to that is 1000 orders for
Report #3.  Those 1000 people send out 5,000 e-mails each for a total of 5
million e-mails sent out.  The 0.2% response to that is 10,000 orders for
Report
#4.  Those 10,000 people send out 5,000 e-mails each for a total of
50,000,000 (50 million) EMails.  The 0.2% response to that is 100,000 orders
for
Report #5.

 THAT'S 100,000 ORDERS TIMES $5 EACH = $500,000.00 (a half million).

 Your total income in this example is:
 1..... $50 +
 2..... $500 +
 3..... $5,000 +
 4..... $50,000 +
 5..... $500,000 ......... Grand Total = $555,550.00

 NUMBERS DO NOT LIE.  GET A PENCIL & PAPER AND FIGURE
 OUT THE WORST POSSIBLE RESPONSES AND NO MATTER
 HOW YOU CALCULATE IT, YOU WILL STILL MAKE A LOT OF
 MONEY!
 REMEMBER FRIEND, THIS IS ASSUMING ONLY 10 PEOPLE
 ORDERING OUT OF 5,000 PEOPLE YOU MAILED.
```

Subject: Do you like pretty little lolitas? Choose your favorite site!
   Date: Fri, 8 Nov 2002 11:07:39 +0100

It's your personal invitation to issue #30 of "THE BEST LOLITAS SITES" magazine.

Are there too many lolitas sites in the Net?

Are you impressed by variety of different suggestions and really don't know what to choose?

And maybe, you're tired from sameness of all that already viewed sites?

Now it is the time to see what sites are now the most actual and outstanding, that can satisy needs of every customer!

Just a few minutes of your time - and you'll understand how the Lolitas industry developed.

The best from the best - just click and choose!

ENTER NOW!!!
ENTER NOW!!!
ENTER NOW!!!
ENTER NOW!!!
ENTER NOW!!!
ENTER NOW!!!
ENTER NOW!!!

```
Subject: Akp İktidarı
   Date: Tue Feb 3 22:13:02 2004
   From: <mhpistanbul@mhp.com>


  KIBRIS POLITIKASI

  Dıs politika konusunda iktidara geldigi günden bu yana vahim hatalar yapan AKP
IKTIDARI 'nın ;

  Kıbrıs konusunda "Çözümsüzlük Çözüm Degildir" söylemiyle Rum tezini destekler
ifade,tutum ve davranıs içinde bulundugunu,

  Avrupa Birligi'nden tarih alabilmek umuduyla Loizidou davasında 1998'den beri
ödenmeyen tezminatı ödeyerek Türkiye 'nin adada isgalci konumda oldugunu zimnen
kabul ettigini,

  Bu kararla Kuzey Kıbrıs Türk Cumhuriyeti 'ni yok saydıgını,

  Türk Ordusuna ve Türk Milletine hakaret etme ve KKTC 'de yapılan seçimlere
dogrudan mudahale etme cüretini gösteren Verheugen 'e sadece eseflerini bildirmekle
kaldıgını,
izledikleri bu tutumla KKTC topraklarının her karısının sehit kanıyla sulandıgını
hatırlamadıgını,

  Biliyor musunuz?

  Milliyetçi Hareket Partisi - ISTANBUL IL BASKANLIGI
```

SPAM Nedir?

- SPAM, çoğunlukla çok fazla sayıda alıcıya gönderilen, talep edilmemiş elektronik iletileri tanımlamak için kullanılan bir terimdir.
- İlk SPAM, 1 Mayıs **1978** tarihinde DEC'in, ABD'nın Batı kıyısındaki tüm ARPANET adreslerine yeni ürünlerini tanıtmak için gönderdiği e-posta olarak kabul edilmektedir.
- İlk ciddi SPAM girişimi ise **1994** yılında iki avukatın kendi hizmetlerini anlatan bir reklam iletilerini USENET'teki 1000'lerce gruba göndermeleri olarak kabul edilir.
- Ayrıca SPAM bir domuz eti konservesinin de markasıdır.
- SPAM e-postaların içerikleri -her zaman olmamakla beraber- genellikle, ürün ya da hizmet pazarlamak gibi ticari amaçlara hizmet eder.

SPAM Nedir?

- Genel olarak aşağıdaki karakteristiklere sahip olurlar:
  - Çoğunlukla alıcıya hiç bir şey ifade emezler.
  - Çirkin ya da yasadışı içerikle gelirler ya da onlara yönlendirirler.
  - İçerikleri yalan ya da yanıltıcı olur.
  - Mesajın başlık bilgileri tahrip edilmiş olur.
  - Alıcıların bu dağıtımdan ileti almak istemediklerini belirtebilecekleri geçerli/fonksiyonel bir adres sunmazlar.
  - Elde edilmesi ve kullanılması kişilik haklarına tecavüz niteliği taşıyan içeriklere sahip olurlar ya da bu yolla toplanan bilgiyi, kitleyi kategorize etmek için kullanırlar.
  - İçeriği tamamen doğru olan ticari e-postalar?

SPAM Nedir?

- SPAM'in tanımı problemi...
  - Üzerinde anlaşılmış bir SPAM tanımı, etkili SPAM karşıtı politikalar geliştirmek için önemli bir ön koşuldur. Internet servis sağlayıcılarının (ISP'lerin) ve yasama otoritelerinin, SPAM yapanlara karşı getirecekleri kısıtlamaların ve yasal hükümlerin ne olacağına karar vermeden önce kabul edilebilir ve kapsamlı bir tanıma ihtiyaçları bulunmaktadır.
  - SPAM için, ISP'lerin, e-posta ile pazarlama endüstrisinin ve kullanıcıların bakış açılarına göre ortak bir tanımlamanın yapılması hayli zor görünmektedir, herkes kendi menfaatlerini koruma gayretindedir.
  - Biz, SPAM'i kullanıcılar ve sistem yöneticileri olarak istenmeyen e-postalar olarak tanımlamaya devam edelim :)

E-posta Adresleri Nasıl Elde Ediliyor?

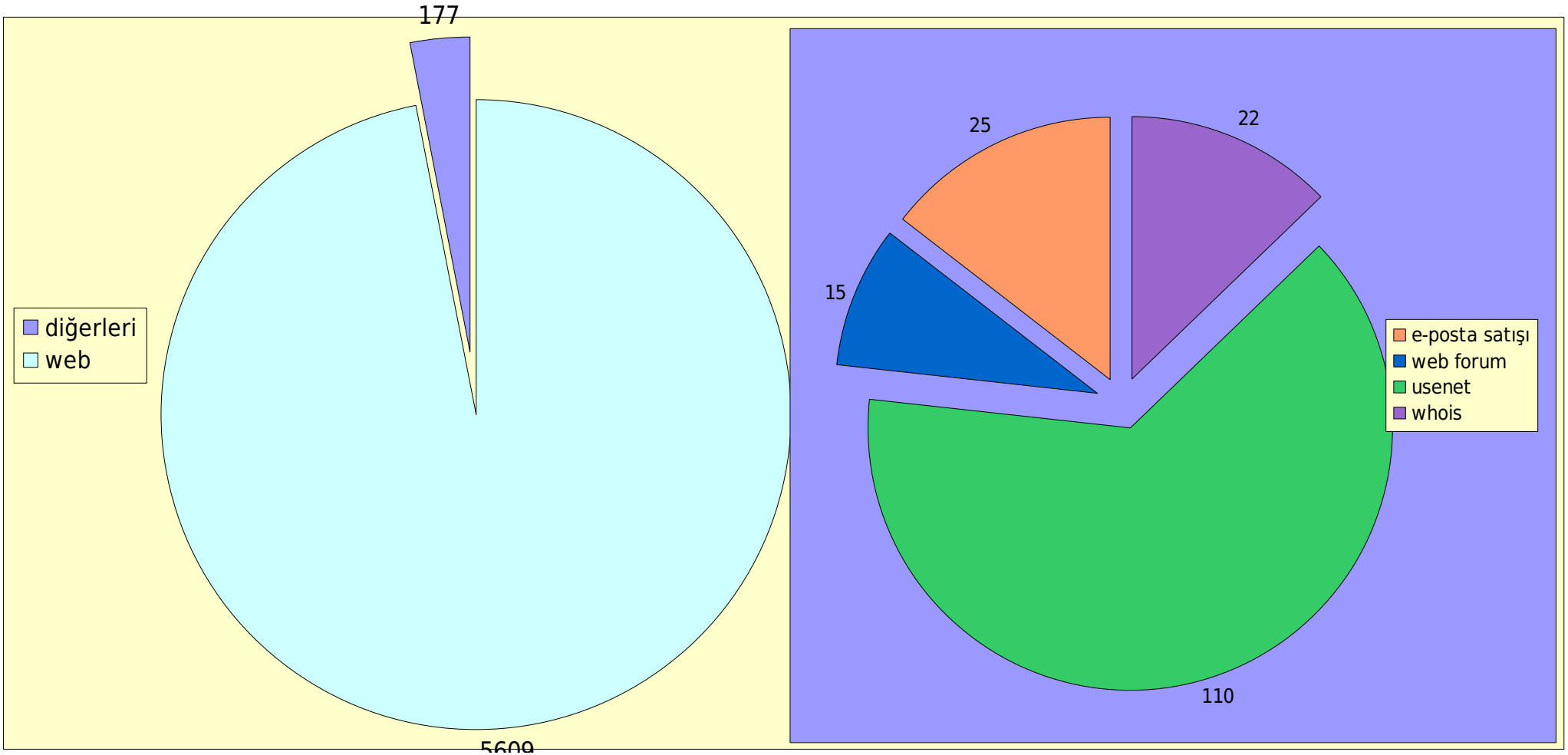
- Web sayfalarından,
- USENET haber gruplarından,
- Web tabanlı tartışma forumlarından,
- Alan adı kayıtlarından (whois çıktılarından),
- E-posta adresi sahiplerinden izinsiz gerçekleştirilmiş e-posta adresi satışlarıdan (şu kadar e-posta adresi şu kadar Lira!)
- Bu kadar mı? Virüsler, Kurtçuk'lar, Chain Mail CC listleri, hatta yetkisiz girilen e-posta sunucusu logları...

E-posta Adresleri Nasıl Elde Ediliyor?

- Hürriyet gazetesinin tirajının 450.116, Milliyet'in tirajının 305.282, Sabah'ın ise 346.422 olduğu bir günde satın alabileceğiniz e-posta sayısı aşağıdaki gibi idi:
  - ~2.000.000 yerli Internet kullanıcısı e-posta adresi: 75$
  - ~5.000.000 yerli Internet kullanıcısı e-posta adresi: 150$
  - ~10.100.000 yerli Internet kullanıcısı e-posta adresi: 300$
  - ~100.000.000 yabancı Internet kullanıcısı e-posta adresi: 100$
  - Kampanyamız süresince e-postaları göndermek için kullanacağınız program da bizden hediye, programlarımız stoklarla sınırlıdır, acele edin! :)

E-posta Adresleri Nasıl Elde Ediliyor?

Aşağıdaki grafik, e-posta adreslerinin nerelerden ele geçirildiğine dair 6 aylık bir araştırmanın bulgularını gösteriyor (IETF, ASRG, 2003).

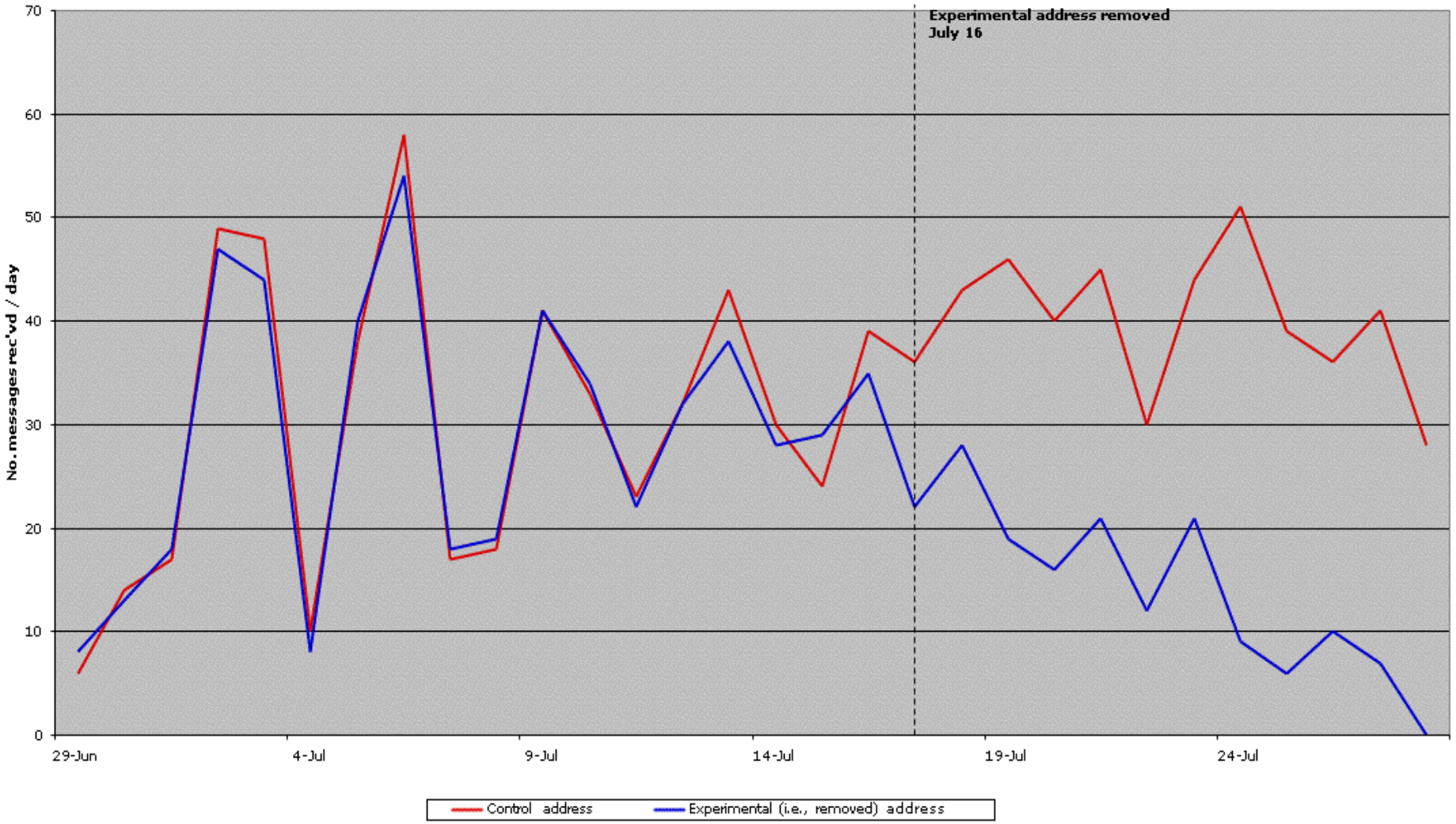


E-posta Adreslerini Koruma Yolları

- Web forumlarda, USENET haber gruplarında, web sitemizde e-posta adreslerini alenen sergilememek:
  - meren~comu.edu.tr
  - meren[at]comu[dot]edu[dot]tr
  - meren@comu.edu.tr
  - adresi küçük boyutlu gif imajları ile görüntülemek
- e-posta adresi seçerken sözlük saldırılarından etkilenmeyecek adresler seçmek.
- http://search.cpan.org/~miyagawa/Apache-AntiSpam-0.05/

E-posta Adreslerini Koruma Yolları

Web sayfasında e-posta adresi bulundurmanın ve bulundurmamanın etkileri:

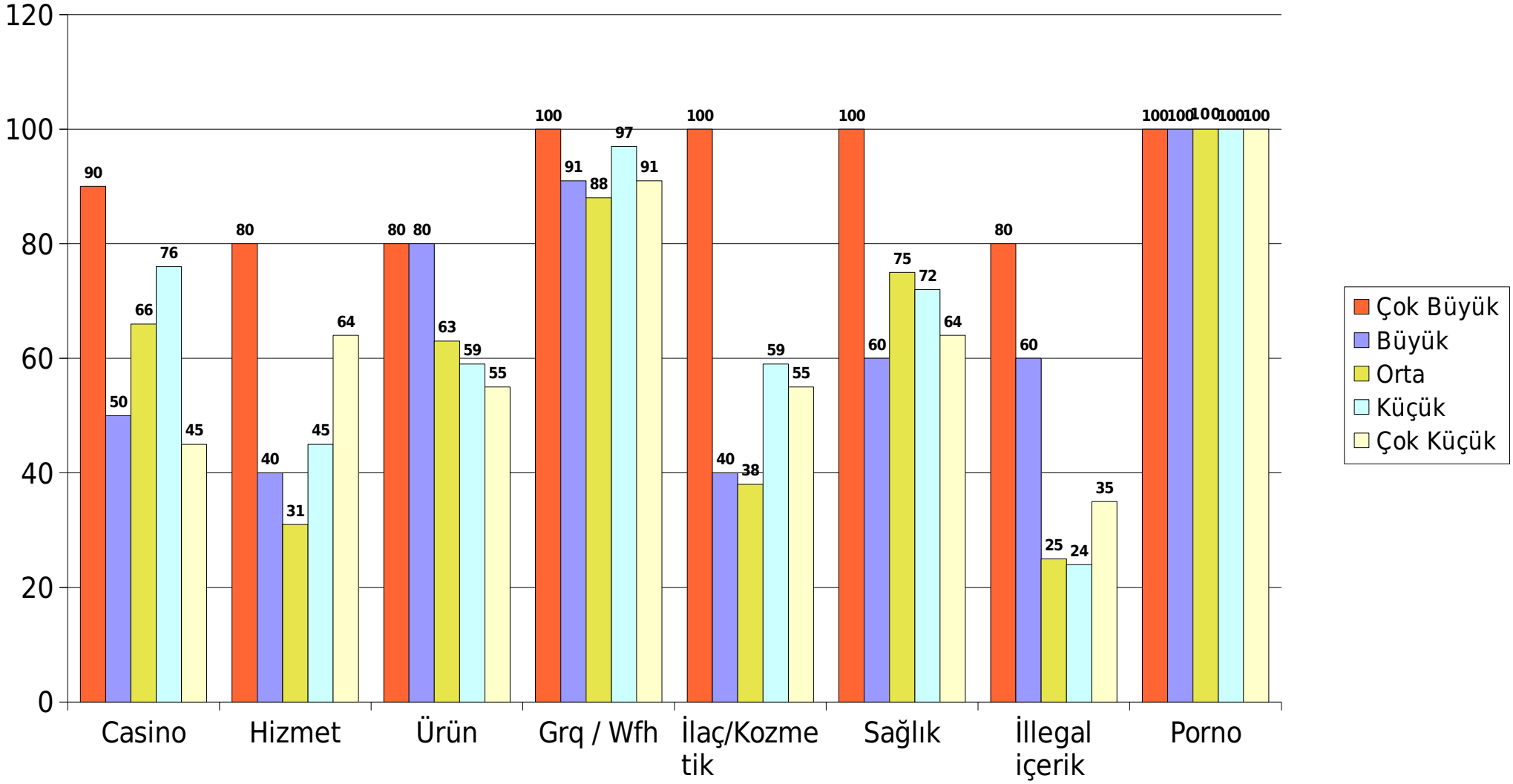


SPAM Hangi İçerikleri Taşır?

- Ürün reklamı (+3″! +5″!!)
- Hizmet reklamı
- Casino'lar (online kumar salonları)
- Hemen zengin ol (get quick rich) / Evinden para kazan
- Sağlık, kozmetik, ilaç (viagra, viagra+, viagra++)
- İllegal içerik (pkk/kadek gibi illegal örgütlenmelerin ajitasyonları v.s.)
- Pornografi

SPAM Hangi İçerikleri Taşır?

ISP'lerin büyük yoğunlukla aldıkları SPAM'lerin içeriklerinin ne olduğuna dair bir araştırmanın sonuçları:



SPAM'in Zararları Nelerdir?

- SPAM genel olarak ayrım gözetmeyen, küresel bir harakettir. Bu özelliği ile SPAM sağduyusuz, yasadışı olan ya da ticari ve yasal olarak sanal ortamın dışında yapılması mümkün olmayan girişimler için popüler bir promosyon aracı haline gelmiştir. Amerika Federal Ticaret Kurulu (FTC) raporuna göre tüm ticari SPAM'lerin yaklaşık %50'si yalan ya da yanıltıcı içeriğe sahiptir. SPAM, hem internet kullanıcılarına, hem internet çalışanlarına hem de yasama otoritelerine meydan okumaya devam etmektedir...

SPAM'in Zararları Nelerdir? (Gizlilik)

- Hangi e-posta adresleri ve hangi kişisel bilgilerin elde edildiği ve biriktirildiği noktasında önemli gizlilik ihlalleri söz konusudur.
- Adres toplayıcılarının internet üzerinden belirli sitelere giren kullanıcıların kişisel bilgilerini ve e-posta adreslerini kendilerinden gizli bir şekilde elde ederek ya da otomatik yazılımlarla tüm interneti tarayarak buldukları e-posta adreslerini biriktirerek oluşturdukları kolleksiyonlarını para ya da karşı tarafın elindeki e-posta adresi birikimi karşılığında e-posta adreslerinin sahiplerinden izin almadan birbirlerine sattıkları çok alışılmış bir durumdur.

SPAM'in Zararları Nelerdir? (İçerik)

- SPAM e-postaların ciddi bir çoğunluğunun içerdiği yasalara aykırı içerik, pornografi, çocuk pornografisi, yasadışı online kumar servisleri, piramit satışlar, hemen zengin olma vaadleri ile aldatıcı ticari eylemler bireylerin psikolojilerini olumsuz yönde etkilemektedir.
- Özellikle toplumun küçük yaştaki mensuplarının Internet'in olumlu özelliklerinden ziyade zararlı yönleri ile tanışmasına neden olmaktadır.

SPAM'in Zararları Nelerdir? (Aldatıcı Eylemler, Spoofing)

- Spoofing, e-posta başlıklarının değiştirilmesi ile iletinin orijinal göndericisi yerine başka bir yerden ya da kurumdan geliyormuş gibi gösterme işlemidir. SPAM yapanlar iletilerinin dikkate alınıp okunması ve cevap verilmesi için spoof yaparak ciddi ve saygın kuruluşların isimlerini kullanabilirler. Bu da kurban seçilen kuruluşların ticari ünlerine zarar getirmekte, zaman ve müşteri kayıplarına yol açmaktadır ve bu durumun düzeltilmesi için yapılan harcamalar kuruma ciddi bir mali yük oluşturmaktadır.

SPAM'in Zararları Nelerdir? (Finansal Tutar)

- SPAM'in sebep olduğu maddi zararın tam değerini hesaplamak elbette mümkün değildir fakat fikir edinmek için elimizde yeterince veri var.
- 2001 yılında Avrupa Birliği'nin yaptığı bir araştırmaya göre tüm dünyada bir yılda meydana gelen SPAM faaliyetlerinin tüm internet kullanıcılarına maliyeti olarak 10 milyar dolar dolaylarında.
- Daha yakın bir tarihte Ferris Research tarafından yapılan bir araştırmanın tahminlerine göreyse sadece Amerikan şirketleri 2002 yılında SPAM'den dolayı 8.9 milyar dolar kayba uğradı, bu miktar Avrupa içinse aynı araştırma şirketi tarafından 2.5 milyar dolar olarak tahmin edildi.

SPAM'in Zararları Nelerdir? (Finansal Tutar)

- Ingiltere'deki çok büyük bir internet servis sağlayıcı olan Star Internet'in verdiği bilgilere göre her bir çalışanının yıllık üretkenliğindeki azalma şirkete çalışan başına 400 dolara mal oluyor.
- Erado'nun spam ile ilgili makalesinde ise spam, virus ve diğer istenmeyen içerikli mesajların neden olduğu yıllık üretim kaybı çalışan başına 1000 dolar.
- IBM'in Almaden Araştırma Merkezi'nin 2001 yılında yaptığı bir araştırma sonucu bir e-posta göndermenin tutarı 0.000082$ (yaklaşık 114 TL) ile 0.000030$ (yaklaşık 37TL) arasında.
- Öte yandan Global Internet Project isimli sitenin tahminine göre bir kişinin spam yapmak için sahip olmasi gereken tek şey olan bir e-posta adresine sahip olmanın tutarı 0.00000032$ (yaklaşık 0.32TL).

2003 Yılı İçin Bazı İç Karartıcı İstatistikler

Dünyadaki e-posta trafiğinin %60'ı SPAM.
Bu da günde 12.4 milyar, yılda 4.5 trilyon SPAM e-posta anlamına geliyor.
Bir günde 2.5 milyar porno içerikli SPAM gönderiliyor.

Bir Internet kullanıcısı günde ortalama 6, yılda ise 2200 SPAM alıyor.

SPAM'ın Internet kullanıcılarına toplam maliyeti 225 milyar dolar.
Internet kullanıcılarının %28'i SPAM dolayısıyla e-posta adresini değiştirmiş.
Kullanıcıların %28'i SPAM iletiyi Reply etmiş.
Kullanıcıların %8'i SPAM yoluyla öğrendiği ürünü satın almış.

1000 çalışanı olan bir şirketin yılda aldığı SPAM 2.7 milyon.
Şirketlerin her bir SPAM ileti için ortalama 9.5 saniye kaybettiği düşünülüyor.
Bu rakamların 2005 yılı için tahmini değişim miktarları %165.

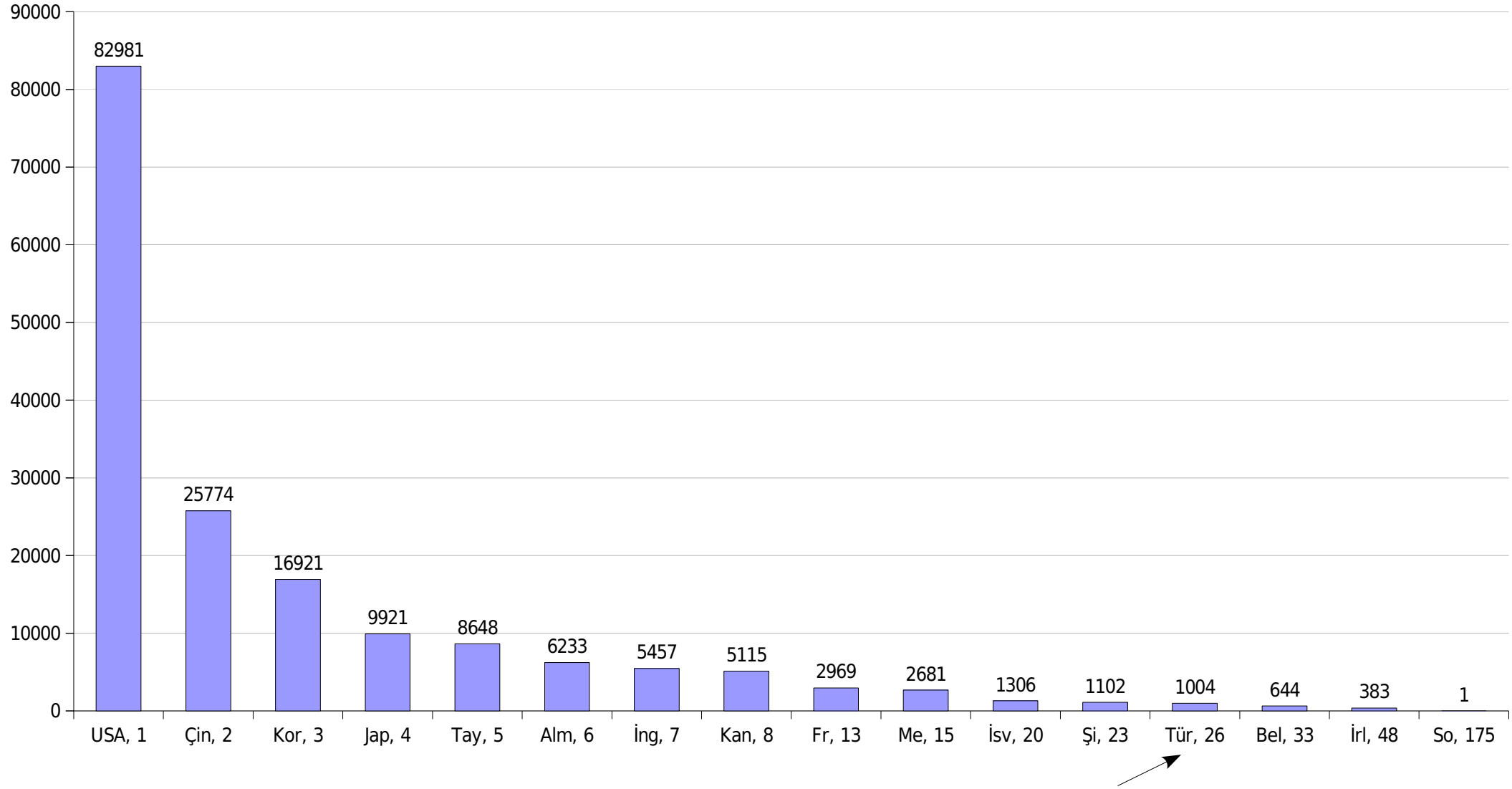
Kaynakça: Google, Brightmail, Jupiter Research, eMarketer, Gartner, MailShell, Harris Interactive ve Ferris Research

Open Relay?

- Open relay, herhangi bir kurumun sistem yöneticisinin Internet'e bağlı olan posta sunucusunu doğru yapılandırmaması sonucu, isteyen herhangi bir kişinin bu sunucu üzerinden dışarıya istediği başlıklarla posta gönderebilmesidir.
- Türkiye dünya çapında bu noktada pek de başarısız görünmemektedir. Yine de sistem yöneticilerinin bilinçlenmesi ve en kısa sürede harekete geçmeleri gereklidir.
- Bilinçlenmek, katkıda bulunmak ve ortak eylem planına hazırlanmak için, http://www.spam.org.tr/'ye göz atmak faydalı olacaktır.

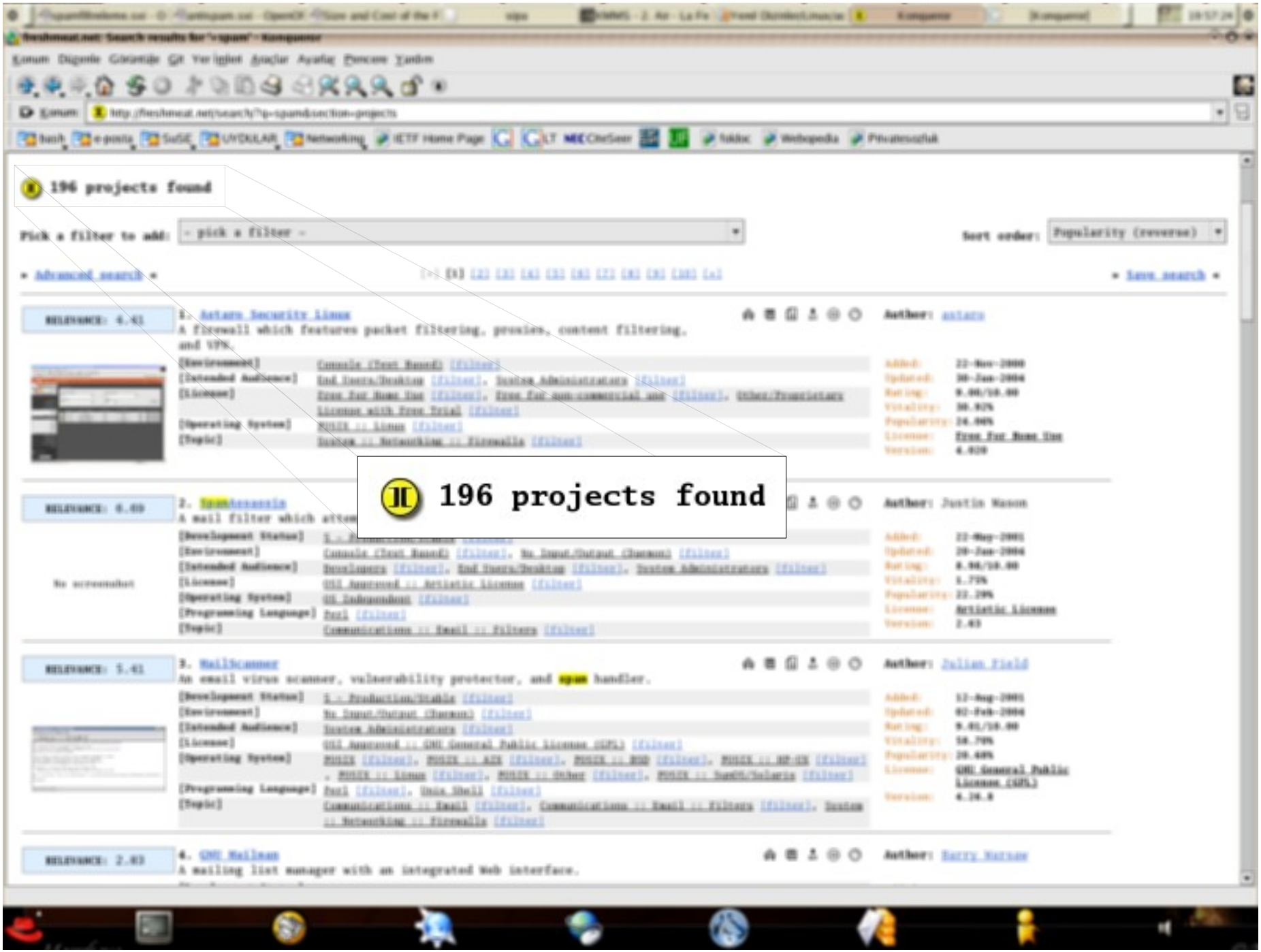
Open Relay ve Türkiyenin Durumu

Open Relay Database, http://www.ordb.org/statistics/countries/, 01/2004



SPAM'i Engellemek İçin Kullanılmış/Kullanılan Yöntemler

- Kalıp Eşleştirme: İçinde şu ya da bu geçiyorsa SPAM'dir.
- Whitelist/Verification: Bu alan bana e-posta atma hakkı olan bir alan mı?
- Dağıtık Blacklist'ler: Bu alan başkaları tarafından karalisteye alınmış bir alan mı?
- Kural Tabanlı Değerlendirme: E-pota içerisinde şu koşul varsa, şu da varsa ve bu da varsa muhtemelen SPAM'dır.
- AI Yaklaşımlar: Bayesian öğrenme metoduna dayalı yöntemler..


196 projects found
196 projects found

RBL Mevzusu

- Realtime Blackhole List
- SPAM kaynağı olduğu kesinleşmiş, RELAY kontrol yapmayan, açık proxy barındıran ya da SPAM araçlarına yataklık ettiği belirlenmiş domain'lerin saklandığı listelerdir.
- Servisten yararlanan posta sunucusu herhangi bir kaynakdan gelen e-postayı kabul etmeden önce RBL veri tabanını sorgular, kaynağın güvenilmez bir kaynak olduğu belirlendiğinde posta kabul edilmez.
- Bütün SPAM'lerin önüne geçilmese de en azında belli başlı kaynaklardan gelenlerin önüne geçilmiş olunur.

RBL Nasıl?

- qmail
  http://www.enderunix.org/documents/qmail.html

- sendmail (native)
  http://www.sendmail.org/~ca/email/doc8.12/cf/m4/anti_spam.html

- postfix (native)
  http://www.postfix.org/uce.html

RBL Nasıl? (qmail)

- rblsmtpd'nin qmail çlıştırdığınız sisteminizde var olması gereklidir.
- rblsmtpd “ucspi-tcp” (UNIX Client Server Program Interface for TCP) paketi ile beraber gelmektedir, bu paketi **http://cr.yp.to/ucspi-tcp/install.html** adresinden temin edebilirsiniz.
  (**ftp://rpmfind.net/linux/contrib/libc6/i386/ucspi-tcp-0.88-1.i386.rpm** adresinde de RPM'si bulunmaktadır.)
- Paket ile ilgili bilgiler ve kurulum notlarına **http://cr.yp.to/ucspi-tcp/ucspi-tcp.html** adresinden ulaşmak mümkündür.

RBL Nasıl? (qmail)

- rblsmtpd'yi qmail'de aktif hale getirmek için **/var/qmail/supervise/qmail-smtpd/run** dosyasında değişiklik yapmanız gereklidir:

```
#!/bin/sh
 qmailDUID=`id -u qmaild`
 NOFILESGID=`id -g qmaild`

 exec /usr/local/bin/softlimit -m 4000000 /usr/local/bin/tcpserver -v -p -H -R -l
0 -x /etc/tcp.smtp.cdb -c 256 -u "$qmailDUID" -g "$NOFILESGID" 0 smtp
/usr/local/bin/rblsmtpd -r relays.ordb.org /var/qmail/bin/qmail-smtpd 2>&1
```

http://www.enderunix.org/

- Artık sunucunuz RBL ile çalışmaya hazırdır. Karalistelerde rastlanan IP adreslerinden gelen e-postalar reddedilecek ve qmail'in log dosyalarına işleneceklerdir.

RBL Nasıl? (sendmail)

- sendmail 8.9.x sürümleri ve üzeri sürümlerinde RBL desteği native olarak bulunmaktadır, RBL'yi aktif hale getirmek için sendmail.mc dosyasına aşağıdaki satırların eklenmesi yeterlidir (elbette aktif hale gelmesi için config dosyasının rebuild edilmesi gereklidir):

```
dnl
FEATURE(`dnsbl', `or.orbl.org', `Spammer $&{client_addr} $&f rejected by RBL: http://www.orbl.org/ (ORBL)')
FEATURE(`dnsbl', `relays.ordb.org', `Spammer $&{client_addr} $&f rejected by RBL: http://ordb.org/ (relays)')
FEATURE(`dnsbl', `list.dsbl.org', `Spammer $&{client_addr} $&f rejected by RBL: http://list.dsbl.org')
FEATURE(`dnsbl', `dnsbl.njabl.org', `Spammer $&{client_addr} $&f rejected by RBL: http://dnsbl.njabl.org')
dnl
dnl
FEATURE(`dnsbl', `proxies.relays.monkeys.com', `Spammer $&{client_addr} $&f rejected by RBL: \
http://proxies.relays.monkeys.com')
dnl
dnl
FEATURE(`dnsbl', `relays.visi.com', `Spammer $&{client_addr} $&f rejected by RBL: http://relays.visi.com')
dnl
FEATURE(`dnsbl', `rbl.spam.org.tr', `Spammer $&{client_addr} $&f rejected by RBL: http://spam.org.tr/rbl')
dnl
```

http://www.Linux-Sec.net/Mail/Sendmail/

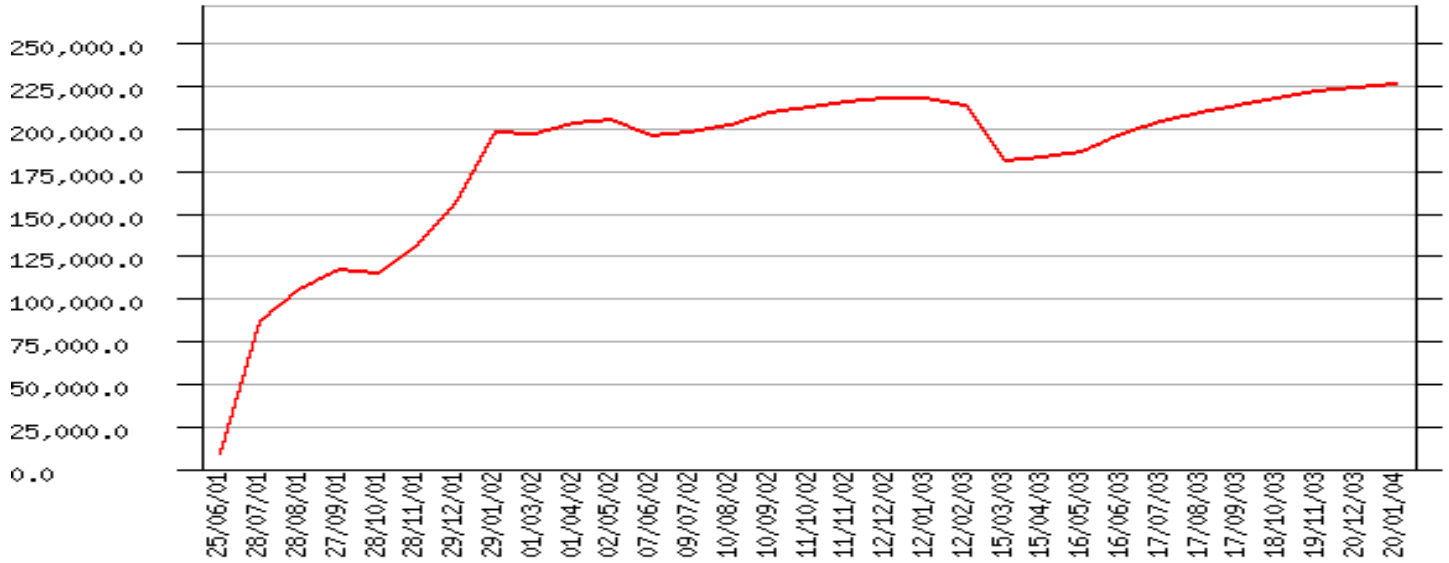
RBL Nasıl? (postfix)

- postfix'te de RBL desteği sendmail gibi native olarak bulunmaktadır. RBL kontrolünü aktif hale getirmek için postfix'in main.cf dosyasına aşağıdaki satırların eklenmesi yeterlidir:

```
maps_rbl_domains =
        blackholes.wirehub.net, dynablock.wirehub.net,
        relays.ordb.org, inputs.orbz.org,
        dialups.relays.osirusoft.com, spews.relays.osirusoft.com,
        or.orbl.org, formmail.relays.monkeys.com,
        proxies.relays.monkeys.com, bl.spamcop.net,
        dialups.relays.osirusoft.com, dnsbl.njabl.org, spamsites.relays.osirusoft.com,
        spamhaus.relays.osirusoft.com, rbl.spam.org.tr
```

RBL Sağlayıcıları

- Open Relay Database (ORDB)
  http://www.ordb.com/



- http://mail-abuse.org, http://www.orbl.org, http://www.spam.org.tr, http://www.orbz.org, http://www.monkeys.com, ...

Kalıp Eşleştirme? Neredeyse İmkansız.

a funny game, a g i n g, a new game, a nice game, a nice game, a virus was detected, a virus was intercepted, abort, accepting credit cards*, accesskey, acne, add length, adilt, adipex, adult, adult material*, adult site*, adult sites*, adult video, adult videos, adu kojo*, adv*, affleck, affordable, affordable health care*, affordable healthcare*, agboola*, age reversal, aging, alert - virus, alimentarios, all information is in the attached file*, all natural ingredients*, all-natural ingredients*, already approved, already wealthy, amazing new discovery*, amazing pranks, an excite game, and you'll save, Angola*, antenna, anti-virus scanner has deleted, antigen found virus, antigen antivirus found virus, antivirus report, anything about anyone, -approved-, approved!, approved medication, approved medications, are so cheap here*, are you an inventor, are you single, artprice, as seen on national television, as seen on tv, at the pump, attachment block message notification, attachment removed, autorizascisn, auto loan, auto loans, auto warranty, babes, bachelor, background searches*, bad credit, bald, baldness, banned CD*, banned C D*, banned filename, bargain, baseball, basketball, be a match, beautiful bride, bedroom satisfaction, benin*, best discount offers, best motorola deal, best prices, best rate, best rates, bestial, better life security, big and bad, big savings, bigger breasts, bigger dick, bigger guys, bigger size, bigger than big, bikini line, biscom*, bitch, bitches, b-i-z, .biz, black worm, bleeding gums, blind date, BLOCKED ATTACHMENT (replaced with text), blocked delivery of email, (blocked subject), blow your load, blowout, blowing, blue pill, boobs, boost+reliability, boyfriend*, bracelet, brain.+.+.+, breaking the habit, breast, breasts, breath tester, breathalyzer*, britney*, broadcast email, bug announcement, bug letter, bug message, bug notice, bulk hosting*, burn fat, business opportunity, buy or sell a home, buy this stock, c'ost, c*o*c*k*s, c*u*m, c0ck, c()ck, cable channel, cable TV, can afford, cannabis, c[illegible]d, cash, cash!, cash for you*, casino*, celeb, celebrities exposed*, cellpadding, cheapest, check it out man, "check it out, man", cherry, child support*, christian, christians, cialagen, cigarette brand, classified ad*, clear skin, click here, click to play video*, clickdrugs, cock*, cocks*, coed, coeds, collect money judgments*, collection judgement, collectors edition, collector's edition, college girls, complementary, computer run raster, comunistas, congratulations, consolidate, copy any DVD movie*, cordless phone, coverage, cr[illegible]it, creditcard, credit card, credit card processing*, credit card!*, credit check, credit rating, credit repair, credit report, credit-profile, creditor, creditors, critical patch, critical update, cruise, cum, cum*, cumming, cumulative patch, cunt, cure employment, curn, current Microsoft critical patch, current Microsoft update, current upgrade, d-e-b-t, D_V_D, d1scounts, dark meat, dating, david to goliath, dear ebay user, dear friend*, de bt, dear future millionaire*, debt, d*e*b*t, debt free, debt reduction, debt relief, de-scramble, de-scrambler, deck of cards, degree, delivery failure, denise, dentist, detected virus, diet, diet pill, diet pills, digital camera, digital sunglasses, detective, did you lose my, diet, diet pills, digita1*, digital pet, digital power filter*, diplomas+university, directtv, directv, directv marketing, discontinued, do not reply, email address, do not send, do not send me, do not send me, document_all.pif, do not delete this*, dont look any further, don't be shy, dollar coin, dollar store, dong, doubleclick.com*, dream date, dream vacation, drugs cost less, dvd backup, earning potential, easy money, earn a college degree, earn a degree, earn big, earn up to, ebay tricks*, e-commerce, e-gift, e-mail marketing*, electric scooter, eliminate your debt, em@il*, email not allowed, enhance, enhanced, enlarge, erotic, erection, error announcement, error letter, escorts, estimado*, estrada*, .eu, every+business+needs, everyone approved*, exciting new, exciting offer, "expand, enlarge, lengthen", explore the lighter side, extended auto warranty, f.ckers, failed to clean virus, failure announcement, failure letter, failure notice, failure report, familynewcomer, fantastic business, fat burning, feel better, feel great, feel young, feel younger, file blocking warning, financial independence, finalist*, financial future, financing, find out more information*, first million*, fitness, fixed rate, flip phone, floodgates, football, FordDirect, forget this address*, foreclosed, foreclosures, found my match, fountain of youth, four reports, freaklest, F_R_, F_R-, F_R_E_E, free!, 'free', free business cards, free cable, free DVD movies*, free gas, free gift, free+installation, free iq test, free money, free movies, free+no obligation*, free pager, free of debt, free phone, free phones, free sample, free shipping, free software, free website hosting*, fresh girls, fresh roasted, "friend,", fu-cks, fu-ck, fu=cked, fuck, fucking*, fukking*, funny game, fwee, gambling*, gamesofvegas, genealogy helper, genuine new-yorker, getaway, get a career, get a degree, get a life, get away, get cash now, get out of debt, get paid to take surveys, get relief, get rid of, get your dish free, gimmicks, girlfriend*, give her something, gobbling, gold double eagle, gold and silver, golf, golfer*, good deal!, gourmet coffee, government grants, great credit card, great deals network*, great jewlery, great price, great savings, great stock, guaranteed, guei*, guess who, h_orny, 'hair, hair', hair removal, hammer is simply*, hard core, hardcore, hardc0re*, hate typing, have heartburn, health at risk, health insurance, herba*, herbalists*, herbs, herbal, here is your chance, hey..., hey boys, hey guy, HGH*, hi-speed media*, high interest, hockey, hola, holiday fun, holiday sale, home bleaching kit*, home business, home-based business, home based business, home document imaging, home employment directory*, home interest rates*, home is worth, homeowner*, homeworkers, honeymoon, horses, hot international opportunity*, hot ladies, hot married women*, hot moms, hot mother, hot stock, hot teens*, hottest, hottest new cell phone*, hot wheel, hot wheels, housewives, how smart are you, HPSC's antivirus/content filter, huge discount, hulk watch, human growth hormone*, I=N=K=J=E=T=S, I have been searching for you!, I have to get the word out*, I like that, immediate release*, I miss you, impotence, improve your job prospects, improve your life, incest, inc-est, increase sales, increased confidence, information you requested, ingreso extra, ink jet, lnstant, insurance, insuran-ce, interest rates, interscan nt alert, instant credit, international+license, internet business directory*, internet crush*, internet security pack, investment, investor, invest, Internet Spy, internet update, invitacion, invitamos, iraq t-shirts, Iron Man*, irs hopes, It's all about keeping in touch, it will cost less, llps, latest net security update, legally, legal+problems, legally ordained*, leonba*, lesbian, lesbians, lesbo, lesbos, lewd, license, life insurance, life-insurance, lips, lip's, list your website*, loan, l@@k, l@@king, long distance, look better, look good, look great, look younger, looking be good, loose weight, loove, l0se, lose inches, lose weight in*, love life, love making, lovemaking, love you, lover, l0ver, low forever, low interest, low-interest, low rates, lower than ever, lowest phone rate*, lowest prices*, lucrative, lust, lusty, luv, macho, mailmarshal has detected a virus, major medical breakthrough, make DVD's, make DVDs, make money*, make love, making money with ebay, mako*, male performance*, manhood, man hunter, many Russian girls, market, marriage saver, Marlboros, masajistas, mass email, master card, MasterCard, master many popular programs, master your pc, masturbation, masterbation, masterbution, masupha ephraim, matchbox, mdaemon warning - virus found, merchant account, matchbox, medication fast, meds, meet people, "men,", microsoft pack, milf, milfs, milf's, millionaire, million united states dollars*, mini camera, mini-vacation*, missing persons, missing valuable skills, MLM, mohammed abacha*, money-making opportunity*, money making opportunity*, money tree*, mortgage*, mrs. sarah rowland*, moving forward!, multi level marketing*, multi-level marketing*, multilevel marketing*, my Ford, my girl, napster, nasty, NAV detected a virus, .name, naughty, nches, ndlovu*, need+funds, nest antivirus system detected, network associates webshield, network pack, network security upgrade, network update, never miss that, new car, "newcomer,", "newcomer!", "newcomer ,", newcomer family history, newcomer@flounder.com, newcomer@pgh.net, newest internet pack, newest microsoft pack, newest microsoft security upgrade, newest net security, newest network upgrade, new hotels, new investment opp, new meds, new microsoft upgrade, new speed tabs, new year's resolution, NFL, nice PDA, nigeria*, nigerian*, ningbo, nkomo*, nkono*, n o r t o n, norton antivirus detected and quarantined, no cost, no cost cell phone, no-cost cell phone, no more doctors, no prescription required, no prior prescription, nokia, Norton system works*, notification from postmaster, nude, o u r, officejet, once in a lifetime*, online business, order today*, opportunity!, opportunity knocks, opt-in*, optin*, oreo, .0rg, orgasm*, OTCBB*, OTCBB:*, O U R, our customers, outdoor gear, overstocked merchandise, ovulation, owoso*, quarantined mail, quit smoking, quit your job, quotes!, r@pe, r@volution, r e g, ra-pe, rape*, rate's, rates are down, rates are going, RC racer, Re: action required for {, Re: approved, re: movie*, Re: details, Re: movies, Re: My details, Re: thank you*, reach millions*, realage, real age, real estate, real man, real money, real relationships with*, realestate, receive future offers*, recover your losses, redbook, reduce travel costs, refill your prescription now, refinance, refinanced, refinancing, r e g, r e g i s t e r, relieve stress, remember that chick, remove fat, removing fat, r e n e w, returned mail:, returned mail: possible virus infection, returned mail: see transcript for details, returned mail: service unavailable, returned mail: user unknown, returned to sender, reumaticas, reunion.com, reward offered, reward will be forfeited, riches, riviera gold, robert allen, rock bottom prices*, rock-bottom prices*, romance, s1ze, s@le, sales, satellite, satisfy her, save big time, save up to, saved me some money, saw your site, schoolgirls, screensaver, s[illegible]/font>curit[illegible]/font>: alerte virus, seks, sekx, sekz, sellecionado, senior citizens, seniors citizens, sensational software, sep ll, sep 1l, sep 1l, serviceteam fotodate*, sewing machine, sex, sex-crazed*, sexy, sexual, 'shape, shape', shlt, sick of deleting spam, sick of spam?, Sierra Leone*, sildenafil, sIuts, size does matter*, size matters, skin tone, sleaze, sleepless, slot jackpots, slut*, sluts*, slutty*, smarter than you think, smartest way, smoking, snewcomerd, snoring, so cool a flash, soccer, software they wanted banned*, sold out, someone special, someone wants to meet you, some people succeed, spam!, spam mail warning notification, spay, special invitation, spending too much, spice girls, spice girl's, .sport, sports, sportsbook.com, s.p.y., stafford loan, stamina, start making money, start yours, start your's, startup cost, stay healthy, stock alert, stock alert:*, stock info, stock+opportunity, stock pick, stock play, stockplay, stockupticks, stop paying, subject: re: your application*, substantial income, suck, suerte, suitesavings, superbowl, super deal, super deals, superkaraoke, support our troops, symantec avf detected, symbol:, system alert (type 1), system works pro, systemworks, v-a-l-i-u-m, v-i-a-g-r-a, v:i:a, v~i~a~g, vacation, vegas, vacation, venture capital, viagara, viagra*, viagra 100mg, viagra+, vicodin, vicq, vioxx, virenalarm*, virus detected, virus detected by network associates, virus encontrado, virus found, virus found in a message you sent, virus in your email, (virus infection), visa, vitamin, vitamins, voice recognition software, böyle gider daha bu :(

%60 - %80 true positive :)

%40 - %50 false positive :((

SpamAssassin

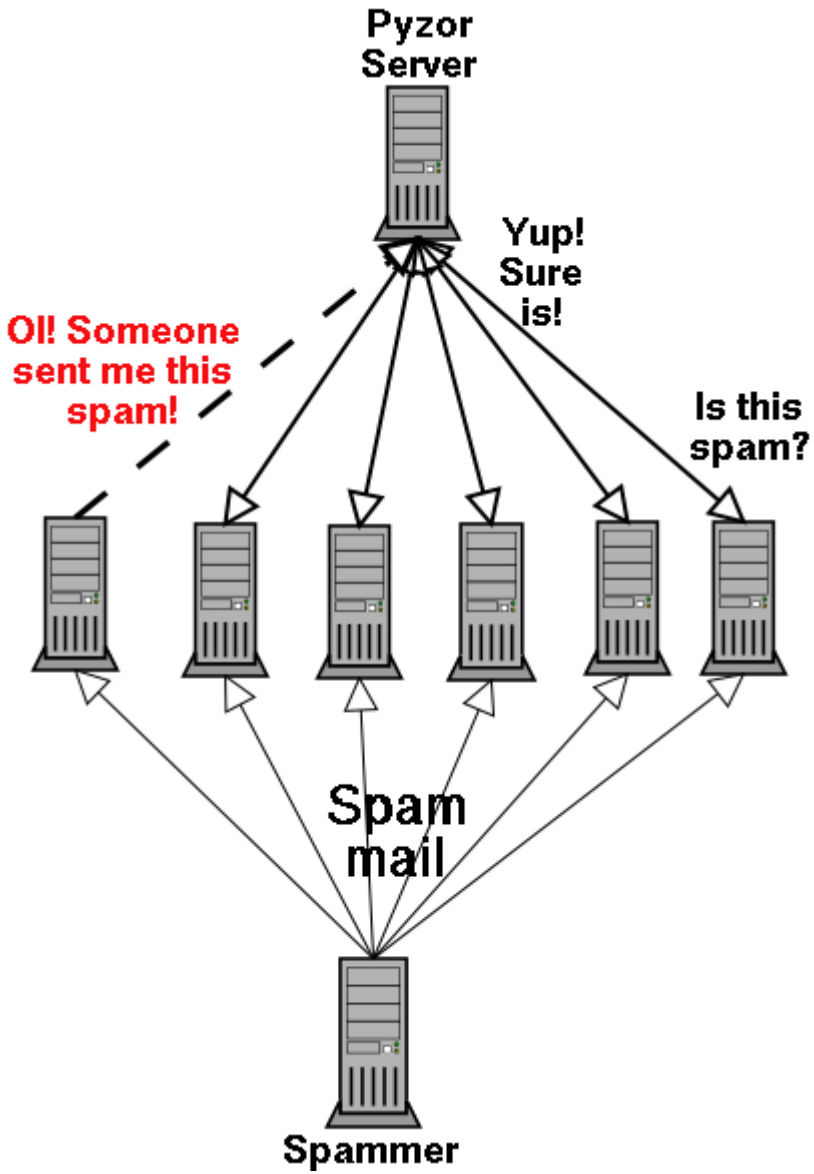
- http://www.spamassassin.org/
- Kural tabanlı (~820 kural) değerlendirme yöntemleri kullanarak bir e-postanın SPAM olup olmadığına karar verir, kural listesi daraltılabilir, genişletilebilir.
- Başarı oranı %95'e kadar çıkabilmektedir.
- sendmail, qmail ve postfix başta olmak üzere neredeyse bütün e-posta sunucuları ile beraber çalışabilir.
- RBL sağlayıcıları ile işbirliği içinde çalışabilir.
- Vipul's Razor, Pyzor gibi SPAM izleme servisleri ile birlikte çalışabilir ve bilikte çalıştırılmaları çok etkili olur, - Perl ile yazıldığından biraz yavaş kalır.

SpamAssassin

- http://wiki.spamassassin.org/w/UsingSpamAssassin
  - SpamAssassin'i qmail, sendmail, postfix gibi e-posta sunucuları ile tümleşik bir şekilde, procmail ile nasıl çalıştırılabileceği ve kullanılabileceğine dair ayrıntılı bilgiler ve linkler içeren bir web sayfası.
- http://www.yrex.com/spam/spamconfig.php
  - SpamAssassin'in local.cf (ya da kullanıcılar için user_prefs) doyasını, bulunmasını istediğiniz özellikleri web arayüzünden seçerek hızlı ve kolay bir şekilde oluşturmanızı sağlayan bir araç.

Pyzor

- http://pyzor.sourceforge.net/
- SPAM iletinin kullanıcılar tarafından tespit edilmesi ve bu iletinin gövde kısmının karakteristiklerinin merkezi Pyzor veritabanına kaydedilmesi metodu ile çalışır.
- Daha sonrasında gelen sorguların da SPAM olup olmadığına öncekilerle karşılaştırarak karar verir, GPL lisansına sahiptir.



Vipul's Razor

- http://razor.sourceforge.net/
- Vipul's Razor da Pyzor gibi dağıtık, kullanıcıların iştiraki ile çalışan bir SPAM belirleme ve filtreleme ağıdır.
- Çalışma prensibi kullanıcıların kendilerine ulaşmayı başarmış bir e-postanın aslında SPAM olduğuna karar verdikten sonra Razor sunucusunu bundan haberdar etmeleri ve aynı e-postanın başkalarına da ulaşmasını engelleme esasına dayanır.
- Bir e-postanın SPAM olduğunun tespiti, istatistiklerin bilinen SPAM içerikleri ile uyuşması yoluyla gerçekleştirilir, fakat GPL lisansına sahip değildir.

Bogofilter

- http://bogofilter.sourceforge.net/
- Eric S. Raymond tarafından yazılmıştır. Bayesian öğrenme metoduna dayalı bir SPAM filtreleme yazılımıdır. (SpamAssassin gibi ilk günden işe yaramaya başlamaz)
- C ile yazıldığından dolayı, hem her sistem ile uyumludur hem de SpamAssassin'e göre çok hızlıdır.

Filtre	*False Positive*	*False Negative*	*Çalışma Süresi (sec.)*
3000 normal e-posta iletisi için			
SpamAssassin	2	250	11900
Bogofilter	0	517	108
5000 linux-kernel e-posta listesi iletisi için			
SpamAssassin	0	6	19600
Bogofilter	0	4	251

- Fakat E. S. Raymod tarafından yazılmıştır. (+fetchmail, +jargon file, -faşizm v.s.)

DSPAM

- http://www.nuclearelephant.com/projects/dspam/
- DSPAM, Bayesian, Chi-Square gibi algoritmaları kullanan bir diğer istatistiksel SPAM filtreleme yazılımıdır.
- Kullanıcıların filtrenin eğitimi için gelen SPAM e-postayı filtreye forward etmeleri yeterlidir.
- Bilinen e-posta sunucularının nerede ise tamamı ile çalışır.
- En son yapılan testlerde %0.07 false positive ürettiği görülmüş başarılı bir filtreleme yazılımıdır.
- C ile yazıldığından dolayı gayet hızlı ve performanslı çalışmaktadır.

Bireysel SPAM Mücadelesi

- Mail Sunucunuzun SPAM filtreleme ile ilgili herhangi bir yatırımı yoksa ve olması da mümkün görünmüyorsa, kendi bilgisayarınızda SPAM filtreleme için de bolca çözüm bulunmaktadır.
- İstemci tarafında SPAM filtreleme için kullanacağınız yazılımlar, sisteminizde perl, fetchmail, procmail gibi neredeyse her sistemde zaten bulunan yazılımların dışında pek bir şey istemeyeceklerdir.
- KMail, Evolution, Sylpheed gibi çok bilinen ve kullanılan e-posta istemcileri ile de rahatlıkla kullanabilirler.

Bireysel Mücadelede A.S.K.

- http://www.paganini.net/ask/
- Active Spam Killer, bir karaliste/kimlik doğrulama uygulamasıdır. Size gönderilen e-postanın geçerli bir sahibi olup olmadığını garanti edene kadar postanın elinize ulaşmamasını sağlar. Bir kez karşıdaki kişinin varlığı teyyid edildikten sonra whitelist'e alınır ve bir daha bu süreç o kişi için işlemez. Ayrıca üye olduğunuz posta listlerini ya da düzenli posta almak istediğiniz adresleri hiç bir işlem yapmadan geçirmesini isteyebilirsiniz. Uzun süre yanıt verilmeyen postalar ise sizin belirlediğiniz bir sürenin sonunda silinirler.
- SPAM'a karşı neredeyse %100 başarı sağlar...

Bireysel Mücadelede A.S.K.

~/.fetchmailrc içerisine:

```
poll mail.comu.edu.tr proto pop3 \
     username meren \
     password m323np455 fetchall
```

~/.procmail içerisine:

```
LOGFILE=$HOME/procmailrc.log
VERBOSE=on

## ASK
:0 fW
|path_to_ask/ask.py --procmail --logfile=$HOME/ask.log --loglevel=10
[bir satir bosluk]
:0 e
/dev/null
[bir satir bosluk]
```

]$ chmod 600 .procmailrc .fetchmailrc

Bireysel Mücadelede A.S.K.

~/.askrc içerisinde satırlar şu şekilde değiştirilir:

```
rc_mymailbox = ontanimli_mailbox_dizininiz
rc_remote_cmd_htmlmail = off
```

fetchmail'in her 10 dakikada bir e-postalarınızı alması için:

```
]$ fetchmail --daemon 600
```

Bu noktadan sonra postalarınız fetchmail ile indirelecek, procmail tarafından da ASK'a borulanacak ve ASK tarafından işlenecektir.

Bu durumda e-posta istemciniz sadece e-postalarınızı göndermek ve mailbox dizininizdeki SPAM'siz e-postaları görüntülemek için kullanacağınız bir araç olacaktır.

Bireysel Mücadelede A.S.K.

(KMail ve Evolution'da yapılması gereken ayarlar)

- KMail: Ayarlar > KMail'i Yapılandır > Ağ > Alma yordamına ekle diyerek “Yerel Posta Kutusu” seçmeli ve yeni pencereden gerekli ayarları yaptıktan sonra kilitleme metodu olarak da FCNTL seçmelisiniz.
- Evolution: Araçlar > Ayarlar > E-posta Hesapları > Ekle'ye kadar geldikten sonra posta alımında sunucu türü olarak “Standart Unix mbox spool or directory” seçmeli, gönderim için de daha önceki gönderim metodunuzu ayarlamalısınız.

Bireysel Mücadelede SpamAssassin (KMail)

- SpamAssassin'i indirin, sisteminizde Perl'in kurulu olduğundan ve ayrıca pod2man'ın da kullanıcınızın path'inde olduğundan emin olun.

```
]$ tar -zxvf Mail-SpamAssassin-2.63.tar.gz
]$ cd Mail-Spamassassin-2.63
]$ perl Makefile.PL PREFIX=~/spamassassin/usr \
>  SYSCONFDIR=~/spamassassin/etc
]$ unset LANG
]$ make && make install
```

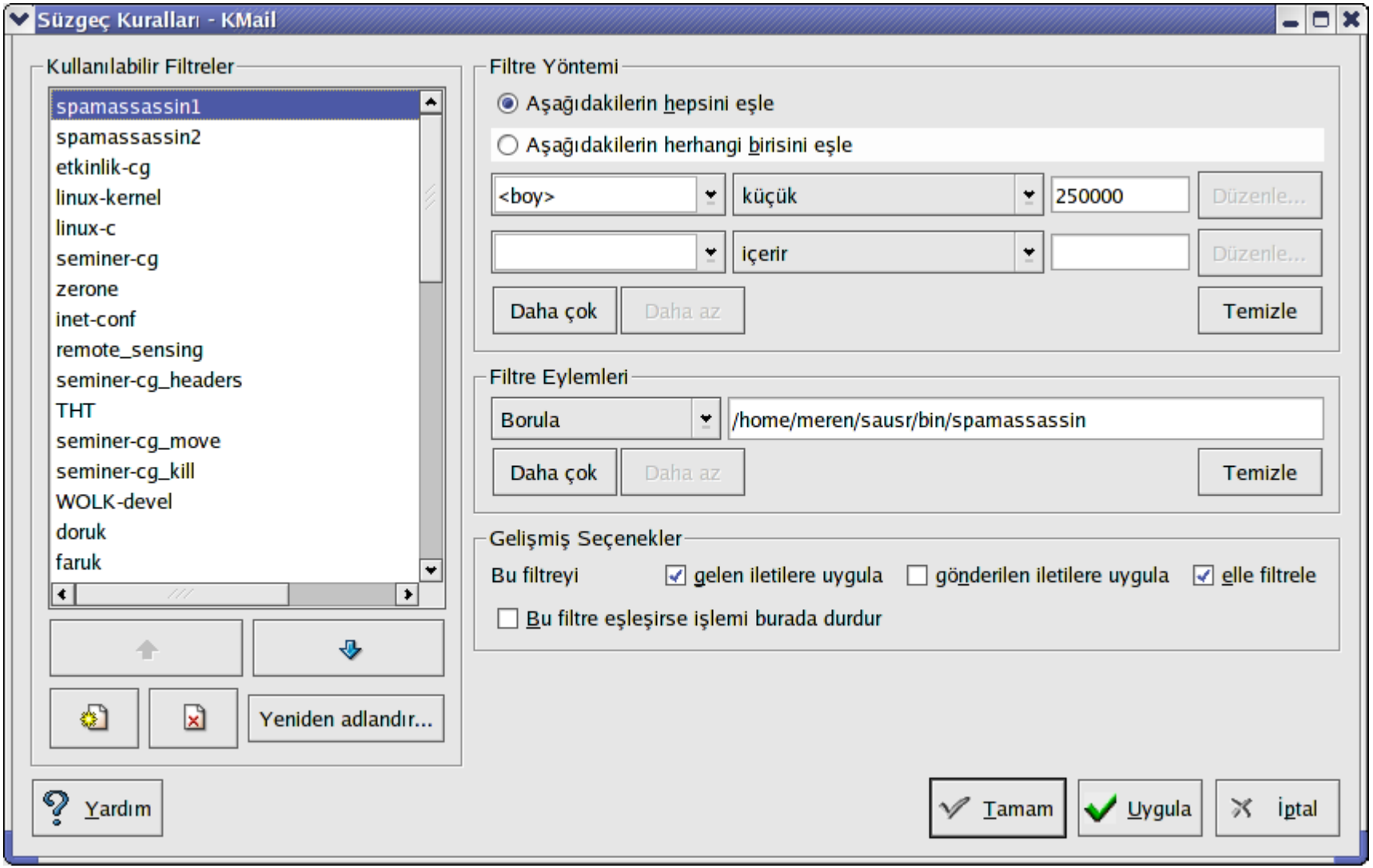
- SpamAssassin'in Bayes ile öğrenmesini istiyorsanız, perl-DB_File yazılımın da sisteminizde bulunup bulunmadığını kontrol ediniz, yoksa kurun.

Bireysel Mücadelede SpamAssassin (KMail)

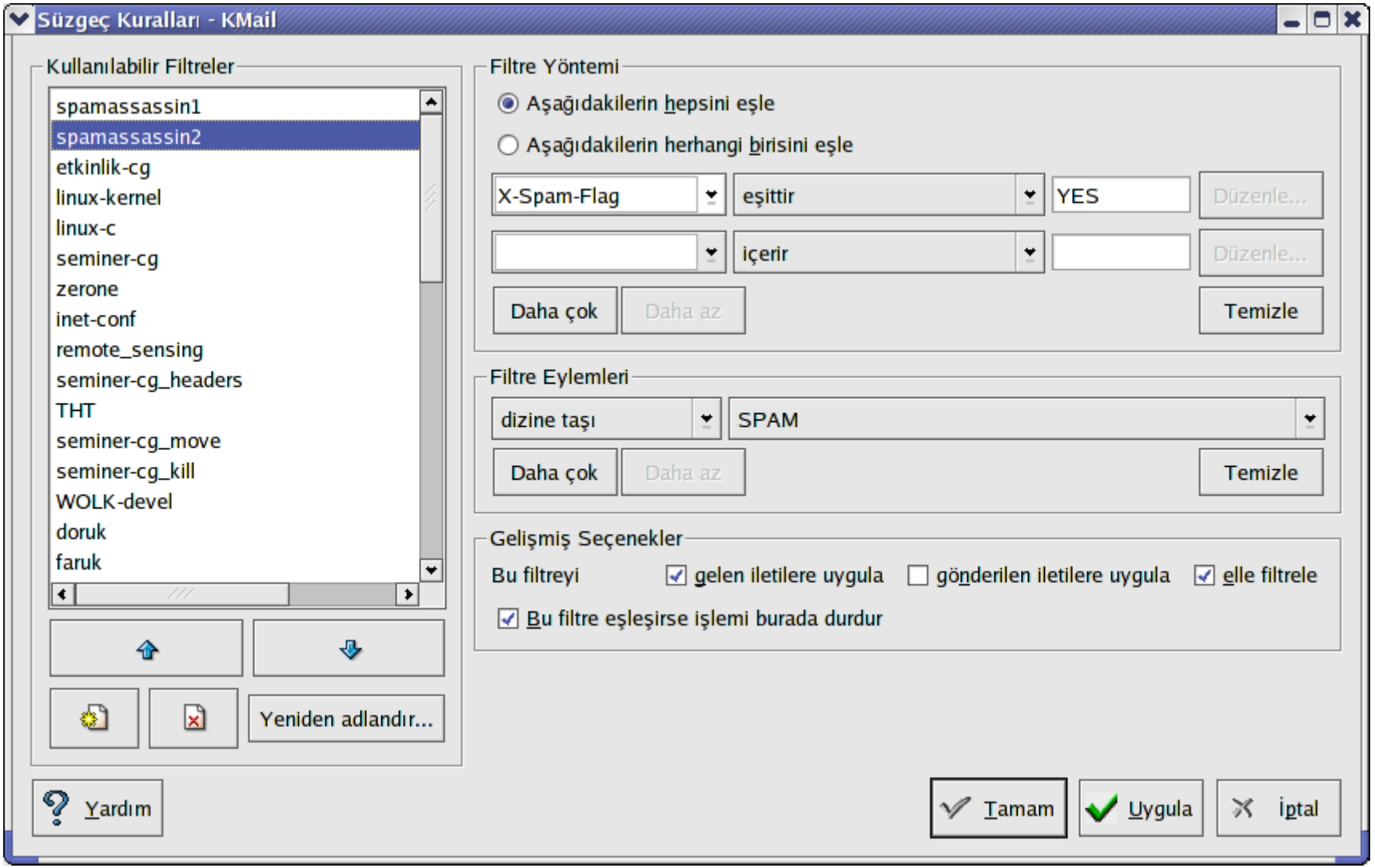
~/spamassassin/etc/mail/spamassassin/local.cf dosyası içerisine,

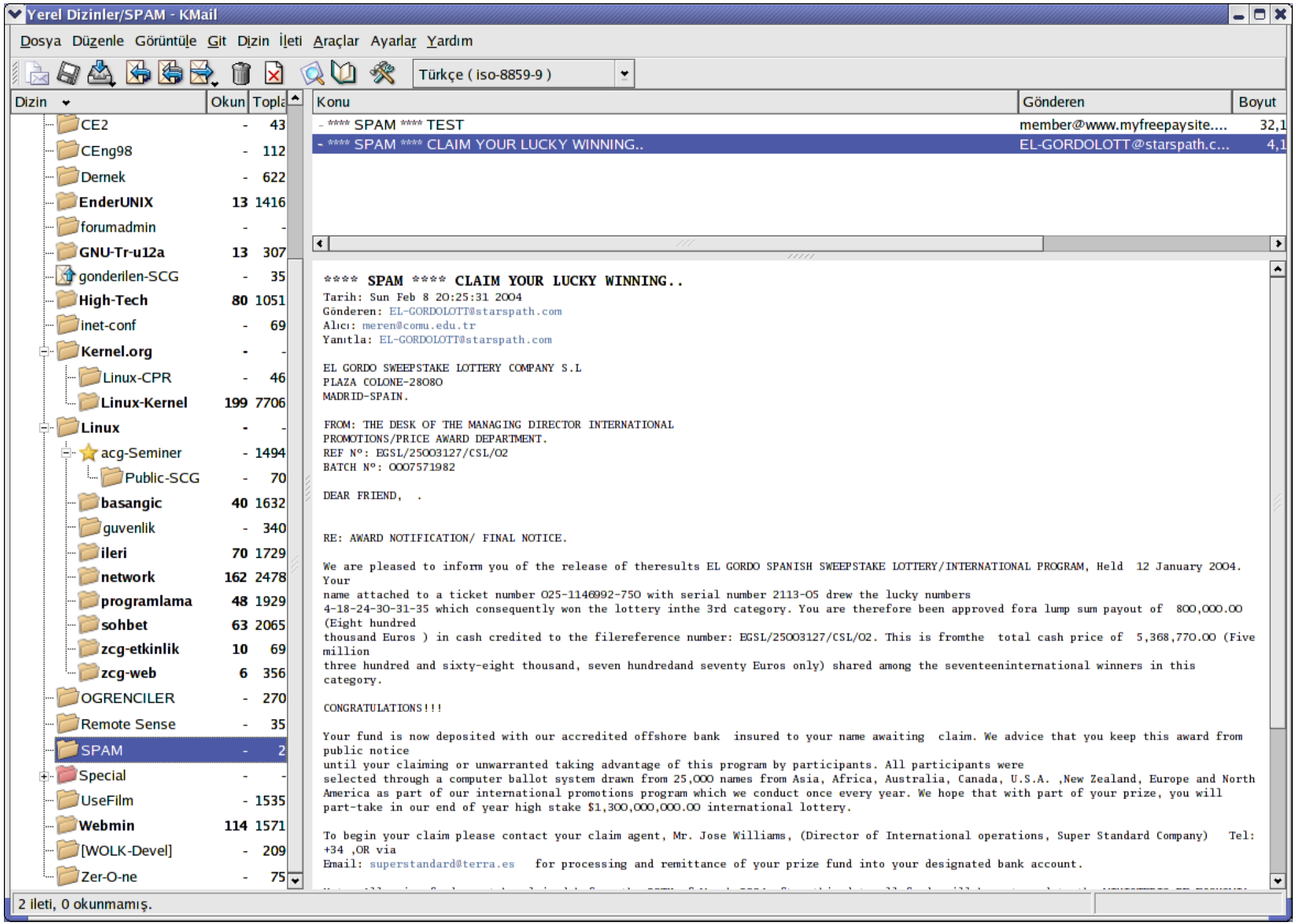
```
required_hits             5
rewrite_subject           1
subject_tag               **** SPAM ****
report_safe               0
use_terse_report          0
use_bayes                 1
auto_learn                1
skip_rbl_checks           1
use_razor2                0
use_dcc                   0
use_pyzor                 0
ok_languages              tr
ok_locales                all

score MICROSOFT_EXECUTABLE    4.0
score SUBJ_ILLEGAL_CHARS      1.0
```

Bireysel Mücadelede SpamAssassin (KMail)



Bireysel Mücadelede SpamAssassin (KMail)




Yerel Dizinler/SPAM - KMail
Dosya Düzenle Görüntüle Git Dizin İleti Araçlar Ayarlar Yardım
Türkçe (iso-8859-9)
Dizin
Okun
Topla
CE2 - 43
CEng98 - 112
Dernek - 622
EnderUNIX 13 1416
forumadmin - -
GNU-Tr-u12a 13 307
gonderilen-SCG - 35
High-Tech 80 1051
inet-conf - 69
Kernel.org - -
Linux-CPR - 46
Linux-Kernel 199 7706
Linux - -
acg-Seminer - 1494
Public-SCG - 70
basangic 40 1632
guvenlik - 340
ileri 70 1729
network 162 2478
programlama 48 1929
sohbet 63 2065
zcg-etkinlik 10 69
zcg-web 6 356
OGRENCILER - 270
Remote Sense - 35
SPAM - 2
Special - -
UseFilm - 1535
Webmin 114 1571
[WOLK-Devel] - 209
Zer-O-ne - 75
Konu
Gönderen
Boyut
**** SPAM **** TEST
member@www.myfreepaysite.... 32,1
**** SPAM **** CLAIM YOUR LUCKY WINNING..
EL-GORDOLOTT@starspath.c... 4,1
**** SPAM **** CLAIM YOUR LUCKY WINNING..
Tarih: Sun Feb 8 20:25:31 2004
Gönderen: EL-GORDOLOTT@starspath.com
Alıcı: meren@comu.edu.tr
Yanıtla: EL-GORDOLOTT@starspath.com
EL GORDO SWEEPSTAKE LOTTERY COMPANY S.L
PLAZA COLONE-28080
MADRID-SPAIN.
FROM: THE DESK OF THE MANAGING DIRECTOR INTERNATIONAL
PROMOTIONS/PRICE AWARD DEPARTMENT.
REF N°: EGSL/25003127/CSL/02
BATCH N°: 0007571982
DEAR FRIEND, .
RE: AWARD NOTIFICATION/ FINAL NOTICE.
We are pleased to inform you of the release of theresults EL GORDO SPANISH SWEEPSTAKE LOTTERY/INTERNATIONAL PROGRAM, Held 12 January 2004. Your
name attached to a ticket number 025-1146992-750 with serial number 2113-05 drew the lucky numbers
4-18-24-30-31-35 which consequently won the lottery inthe 3rd category. You are therefore been approved fora lump sum payout of 800,000.00 (Eight hundred
thousand Euros) in cash credited to the filereference number: EGSL/25003127/CSL/02. This is fromthe total cash price of 5,368,770.00 (Five million
three hundred and sixty-eight thousand, seven hundredand seventy Euros only) shared among the seventeeninternational winners in this category.
CONGRATULATIONS!!!
Your fund is now deposited with our accredited offshore bank insured to your name awaiting claim. We advice that you keep this award from public notice
until your claiming or unwarranted taking advantage of this program by participants. All participants were
selected through a computer ballot system drawn from 25,000 names from Asia, Africa, Australia, Canada, U.S.A. ,New Zealand, Europe and North America as part of our international promotions program which we conduct once every year. We hope that with part of your prize, you will part-take in our end of year high stake $1,300,000,000.00 international lottery.
To begin your claim please contact your claim agent, Mr. Jose Williams, (Director of International operations, Super Standard Company) Tel: +34 ,OR via
Email: superstandard@terra.es for processing and remittance of your prize fund into your designated bank account.
2 ileti, 0 okunmamış.

Son Sözler...

- E-posta adreslerinin ortalarda dolaşmamasına herkes özen göstermek durumundadır. Sadece kendi e-posta adresi için değil, başkalarınınki için de...
- SPAM ile bireysel olarak savaşmaktan ziyade bir çok kişinin ortak mücadelesi için oluşturulmuş çözümlere kulak kabartmak gereklidir...
- E-posta sunucularının izinsiz relay'e izin vermemesi için gerekli düzenlemenin yapılması şarttır.
- RBL'lerde yer alan ip adreslerinden gelen hiç bir e-posta ağa girememelidir, SPAM'a karşı en azından bu yapılmalıdır.

Son Sözler...

- RBL + Pyzor + SpamAssassin güçlü bir çözümdür ve ulusal SPAM politikalarına adapte olabilmek için gereken altyapıyı sağlayabilir görünmektedir.
- http://www.spam.org.tr/ adresi Türkiye Anti-SPAM Organizasyonu'nun çalışmalarına ulaşmak ve yeniliklerden haberdar olmak için sıklıkla ziyaret edilmelidir.
- Aynı şekilde anti-spam e-posta listesini takip etmek kişilerin çözümlerini öğrenmek ve yeniliklerden haberdar olmak için iyi bir yoldur.

To: ecartis@inet.net.tr, Subject: subscribe anti-spam

Kaynaklar...

http://www.geocities.com/spamresources/spamlinks.htm
http://www.linuxfocus.org/Turkce/January2003/article279.shtml
http://www.spamassassin.org/
http://pyzor.sourceforge.net
http://www.spamhaus.org/
http://listweb.bilkent.edu.tr/anti-spam/
http://www.spam.org.tr/
http://www.sendmail.org/
http://www.ordb.org/
http://www.nuclearelephant.com/projects/dspam/
http://www.linux-sec.net/Mail/AntiSpam/
http://www.google.com/
...

Teşekkürler...

Bu sunumun slaytlarına,
http://seminer.linux.org.tr/seminer-notlari/spamfiltreleme.sxi
adresinden ulaşabilirsiniz.

A. Murat Eren
meren~comu.edu.tr
http://zion.comu.edu.tr/~evreniz/