T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

SPAM İLETİLERİN İNTERNET OMURGASINA YAN ETKİLERİ VE ENGELLENMESİ

YÜKSEK LİSANS TEZİ

KEMAL UZUN

İSTANBUL 2009

T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

SPAM İLETİLERİN İNTERNET OMURGASINA YAN ETKİLERİ VE ENGELLENMESİ

YÜKSEK LİSANS TEZİ

KEMAL UZUN

TEZ DANIŞMANI
Dr. RİFAT ÇÖLKESEN

NİSAN 2009
İSTANBUL

TEŞEKKÜR

Bugüne kadar bana her türlü desteği veren ve yardımlarını esirgemeyen sevgili aileme, tez çalışmam süresince değerli vaktini harcayarak bana yol gösteren ve yardımcı olan danışmanım Dr. Rifat ÇÖLKESEN'e teşekkür ederim.

YEMİN METNİ

Sunduğum yüksek lisans tezini akademik etik ilkelerine bağlı kalarak, hiç kimseden akademik ilkelere aykırı bir yardım almaksızın bizzat kendimin hazırladığına and içerim.

25.05.2009

Kemal Uzun

T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜ
TEZLİ YÜKSEK LİSANS TEZ SINAV TUTANAĞI

25/05/2009

Enstitümüz Bilgisayar Mühendisliği Anabilim Dalı Bilgisayar Mühendisliği Bilim Dalı yüksek lisans öğrencilerinden 060820004 numaralı ***Kemal UZUN' a*** *"Beykent Üniversitesi Lisansüstü Eğitim - Öğretim Yönetmeliği"*nin ilgili maddesine göre hazırlayarak, Enstitümüze teslim ettiği ***"SPAM İLETİLERİN İNTERNET OMURGASINA YAN ETKİLERİ VE ENGELLENMESİ"*** *tezini*, Yönetim Kurulumuzun 30.04.2009 tarih ve 2009/05 sayılı toplantısında seçilen ve Fakülte binasında toplanan jüri üyeleri huzurunda, ilgili yönetmeliğin *(c) bendi gereğince* aday tarafından savunulmuş ve sonuçta adayın tezi hakkında ***oybirliği*** ile ***Kabul*** kararı verilmiştir.

İşbu tutanak, 4 nüsha olarak hazırlanmış ve Enstitü Müdürlüğü'ne sunulmak üzere tarafımızdan düzenlenmiştir.

DANIŞMAN
YRD. DOÇ. DR. Rifat ÇÖLKESEN

ÜYE
Prof. DR. Yahya KARSLIGİL

ÜYE
Prof. Dr. Esat HAMZAOĞLU

ÖZET

SPAM İLETİLERİN İNTERNET OMURGASINA YAN ETKİLERİ VE ENGELLENMESİ

KEMAL UZUN

2009

Günümüzde sürekli gelişen ve kullanımı artan İnternet teknolojileriyle birlikte e-posta kullanımı, haberleşmenin en önemli araçlarından biri haline gelmiştir. Çok kısa bir sürede milyonlarca kişiye ulaşılabilecek kadar popüler olan e-posta haberleşmesinin zamanla ticaret, SPAM, saldırı ve virüs gibi eylemlerin odağı haline gelmesi kaçınılmaz olmuştur. Gündelik hayatımızın bir parçası haline gelen e-posta trafiğinin büyük bir kısmını oluşturan SPAM e-postalar, hem kullanıcıları hem de İnternet trafiğini önemli ölçüde meşgul etmektedir.

Bu çalışmada öncelikle SPAM e-postaların sebep olduğu olumsuzluklar ele alınmış olup, SPAM e-posta gönderme teknikleri ve SPAM e-postaların engellenmesi konusunda derinlemesine araştırmalar yapılmıştır. SPAM e-postaların engellemesine yönelik kullanılan teknikler detaylı bir şekilde açıklanarak, e-posta sunucusunda ve kullanıcı tarafında yapılan uygulamalarla ortaya çıkan sonuçlar değerlendirilmiştir.

Bu çalışmadaki teknik uygulamalar, yapılandırmalar, sonuç ve çözüm önerileri, spam e-postaların engellenmesi konusuna ışık tutacaktır.

Anahtar Kelimeler: SPAM, İstenmeyen e-posta, SPAM ileti, Junk e-posta, SPAM e-postaların engellenmesi.

Tez Danışmanı: Dr. Rifat ÇÖLKESEN

ABSTRACT

SIDE EFFECTS OF SPAM MESSAGES OVER WEB SPINE AND BLOCK ACTIVITY

KEMAL UZUN

2009

E-mail usage, together with the continuous development and usage of Internet Technologies, has became one of the most important components of the communication area. In a very short period of time, it is unavoidable to be focussed. E-mail communication which became most populer to be reached to the millions of people has became unavoidable and attracted the attention of the the trade, SPAM, attack and virus activities. SPAM e-mails which are the major part of the e-mail traffic considerably employs the users and the Internet traffic at the same time.

In this thesis, it is dealth with primarily the negative effects of the SPAM and e-mail messages and studies of block of e-mail and SPAM mail sending techniques are also deeply considered. The techniques blocking the SPAM messages and the results arising from the usage of applications in the e-mail server are explained and evaluated in a very detailed way.

The technical applications, configurations, results and the suggestions of the solutions used in this thesis will show the way to block the SPAM mail messages.

Key Words: SPAM, unwanted e-mail, SPAM message, junk e-mail, blocking of SPAM e-mails

Advisor: Dr. Rifat ÇÖLKESEN

İÇİNDEKİLER

KISALTMALAR LİSTESİ

A	Address
APWG	Anti Phishing Work Group
ASCII	American Standard Code for Information Interchange
CAN-SPAM	Controlling the Assault of Non-Solicited Pornography and Marketing
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
DCC	Distributed Checksum Clearinghouse
DNS	Domain Name System
HTML	Hyper Text Markup Language
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPSec	Internet Protocol Security
ISP	Internet Service Provider
Malware	Malicious Software
MAPS	Mail Abuse Prevention Systems
MRTG	Multi Router Traffic Grapher
MMF	Make Money Fast
MIME	Multipurpose Internet Mail Extensions
MX	Mail Exchange
NS	Name Server
OCR	Optical Character Recognition
POP	Post Office Protocol
PUP	Potentially Unwanted Programs
RBL	Realtime Black List
RFC	Request For Comments
SMTP	Simple Mail Transfer Protocol
RMX	Reverse Mail Exchanger
SPEWS	Spam Prevention Early Warning System
SPF	Sender Policy Framework
RSS	Relay Spam Stopper
UBE	Unsolicited Bulk E-mail
UCE	Unsolicited Commercial E-mail
URL	Uniform Resource Locator
TCK	Türk Ceza Kanunu
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/ Internet Protocol
TK	Telekomünikasyon Kurumu

ŞEKİL LİSTESİ

1. GİRİŞ

Günümüzün en önemli iletişim araçlarından biri haline gelen e-posta kullanımının yaygınlaşmasına paralel olarak, e-posta sisteminin içinde barındırdığı SPAM, virüs, saldırı gibi tehditler de sürekli artmaktadır.

Genellikle güvenilmeyen ürünlerin tanıtıldığı reklam niteliğindeki SPAM e-postalar, tüm e-posta trafiğinin çok önemli bir kısmını oluşturmaktadırlar. SPAM e-postalar, SPAM gönderici açısından çok küçük bir harcama ile gerçekleştirilebilirken mali yük büyük ölçüde e-posta alıcıları veya servis sağlayıcı kurumlar tarafından karşılanmak zorunda kalınmaktadır. SPAM e-posta trafiğinin harcadığı bant genişliği ile kullanıcıların uğradığı vakit ve verimlilik kayıpları açısından mali yük önemli boyutlara ulaşmaktadır. SPAM e-postaların engellenmesi, bu yükü ortadan kaldırmak için önemli olduğu kadar, SPAM e-postalarla yayılan phishing, virüs, trojan gibi kötü amaçlı yazılım içeriğinin de önüne geçmek açısından son derece önemlidir.

Bu çalışmada SPAM e-postaların oluşturduğu trafik ve SPAM e-posta gönderme teknikleri analiz edilerek SPAM e-postaların engellenmesine yönelik yöntemler ele alınmış ve bu yöntemlerin bir sunucuda uygulaması yapılmıştır.

Bu tez çalışması altı bölümden oluşmaktadır. E-posta sisteminin temel çalışma prensiplerinin anlatıldığı ikinci bölümü, SPAM e-posta trafiğinin ve sisteminin detaylı bir şekilde yer aldığı üçüncü bölüm takip etmektedir. Dördüncü bölümde SPAM e-postaların engellenme yöntemleri ele alınmış olup bu yöntemlerin kurumsal bir sunucudaki uygulamasına 5. bölümde yer verilmiştir. Tespit ve önerilerin sunulduğu sonuç bölümüyle çalışma bitirilmiştir.

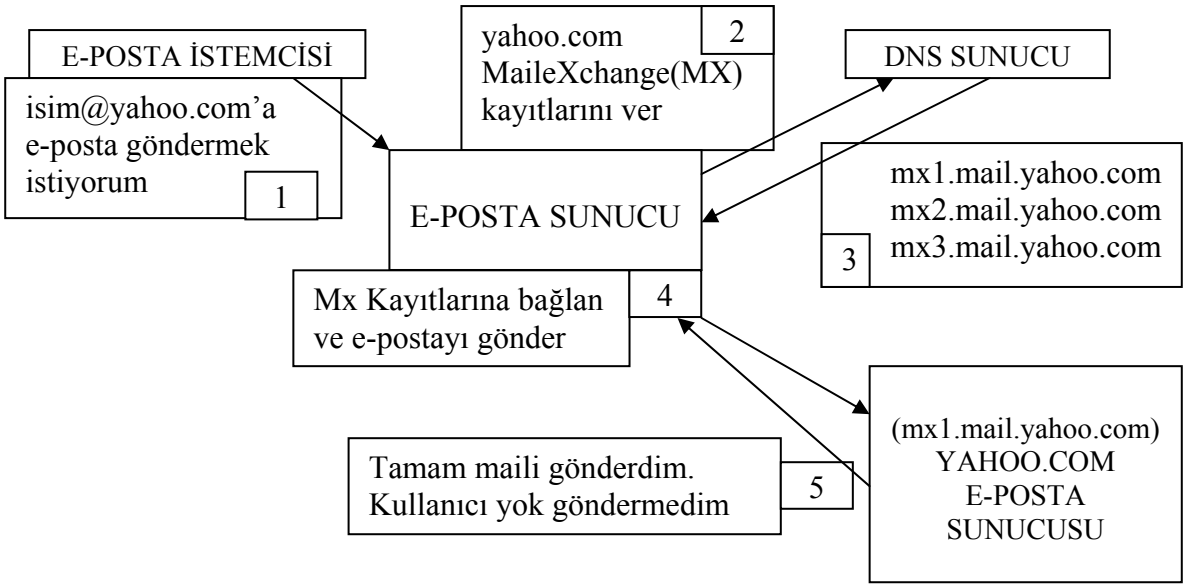
2. E-POSTA SİSTEMİ

2.1. Elektronik Posta (E-posta)

E-posta olarak kısaltılan elektronik posta, kullanıcıların sayısal iletişim sistemleri vasıtasıyla yazdıkları ve birbirlerine gönderdikleri iletilere verilen adlandırmadır.[3]

E-posta gönderimi, TCP/IP uygulama katmanında yer alan ve RFC 821 standardıyla oluşturulmuş olan SMTP(Bölüm 2.2.) protokolüyle sağlanır. Gelen e-postalara erişimi sağlayan protokoller ise, RFC 918 standardıyla oluşturulmuş POP (Post Office Protocol) ve RFC 1730 standardıyla oluşturulmuş IMAP (Internet Message Access Protocol) protokolleridir.

E-posta sisteminin çalışma mantığı basit bir biçimde Şekil 1'de ifade edilmiştir.



Şekil 1 – Tipik Bir E-posta Sistemi Bileşenleri[4]

1. Öncelikle e-posta sunucu istemciden e-posta gönderme isteği geldiğinde bunu kabul eder.
2. E-posta sunucusu alıcının alan adına (domain'ine) ait MaileXchange kayıtlarını DNS sunucudan ister.
3. DNS sunucu cevabını gönderir.

4. E-posta sunucu öğrenmiş olduğu MX kayıtlarına ait IP kayıtlarına bağlanır. Bu IP adresleri karşı sunucunun IP adresleridir.
5. Bağlantı kurulduktan sonra e-posta isteği gönderilir. Karşı taraf alıcı gerçekten varsa bunu kabul eder. Yoksa ya da kota aşımı gibi durumlar söz konusuysa bunu hata kodu olarak geri gönderir. [4]

2.1.1. E-posta Mesaj Formatı

E-posta mesaj formatı, 1982 yılında oluşturulan RFC 822 standardı ile sadece ASCII metin içerikli kullanımı desteklerken, 1992 yılında RFC 1341 standardı ile oluşturulan ve 1996 yılında RFC 2045 standardı ile güncellenen MIME (Multipurpose Internet Mail Extensions -çok amaçlı İnternet posta uzantıları) ile birlikte, içinde kompozit yapıların (resim, ses, video, html dökümanları, çalışabilir program vb) ekli olduğu e-postaların kullanımı mümkün hale gelmiştir. [2]

E-posta, başlık (header) ve gövde (body) olmak üzere iki kısımdan oluşur. Başlık gövdeden boş bir çizgi ile ayrılır.

Başlık (Header); Kimden (From), Kime (To), Bilgi (CC), Gizli (BCC), Tarih (Date), Konu (Subject), Alındı (Received) ve Message-ID bilgilerini içerir. Bir e-postanın alıcıya doğru yola çıkmasından itibaren, e-postanın geçmiş olduğu sunucular tarafından mesaj başlığına "Received" satırları eklenir ve bu satırlar e-postanın geriye dönük izlenmesine olanak tanıması açısından önemlidir.

Gövde (Body) kısmı ise e-posta mesajının metin ve Ek(Attachment) bilgilerinden oluşur. "Attachment", yazıya ek olarak yollanan dosyalardır. Mesaj içeriği ve dosyalar eklenmeden önce base64, Quoted-Printable gibi metotlarla kodlanırlar. Ses, resim, video, yazı başta olmak üzere birçok değişik formatta dosya eklenebilir. [3]

E-posta mesaj başlığındaki İçerik Aktarım Kodlaması (Content-Transfer-Encoding), İçerik Türü (Content-Type) gibi ilave satırlar MIME içerik bilgisini verir.

```
From: kemal@kemaluzun.com.tr
To: rasit@rasitokudan.com.tr
Subject: Picture.
MIME-Version: 1.0
Content-Transfer-Encoding: base64
Content-Type: image/jpeg

base64 encoded data .....
.....
.....base64 encoded data
```

Şekil 2 – MIME

MIME sürümünün 1.0 olduğu Şekil 2'de, "Content-Transfer-Encoding" veriyi çözmek için kullanılan metodu bildirir. "Content-Type" satırı, mesaj gövde ve ek veri tipinin image/jpeg olduğunu belirtmekte olup, "Base64 encoded data…" satırı çözülmüş veriyi ifade etmektedir.

Kullanılan diğer içerik türleri multimedia veri tipleri, Text(düz(plain), html), Image(jpeg, gif), Audio (basic (8 bit mu-law encoded), 32kadpcm (32 kbps coding)), Video(mpeg, quicktime) ve Applications (msword, zip, octet-stream) şeklinde ifade edilebilir.

2.2. SMTP (Simple Mail Transfer Protocol)

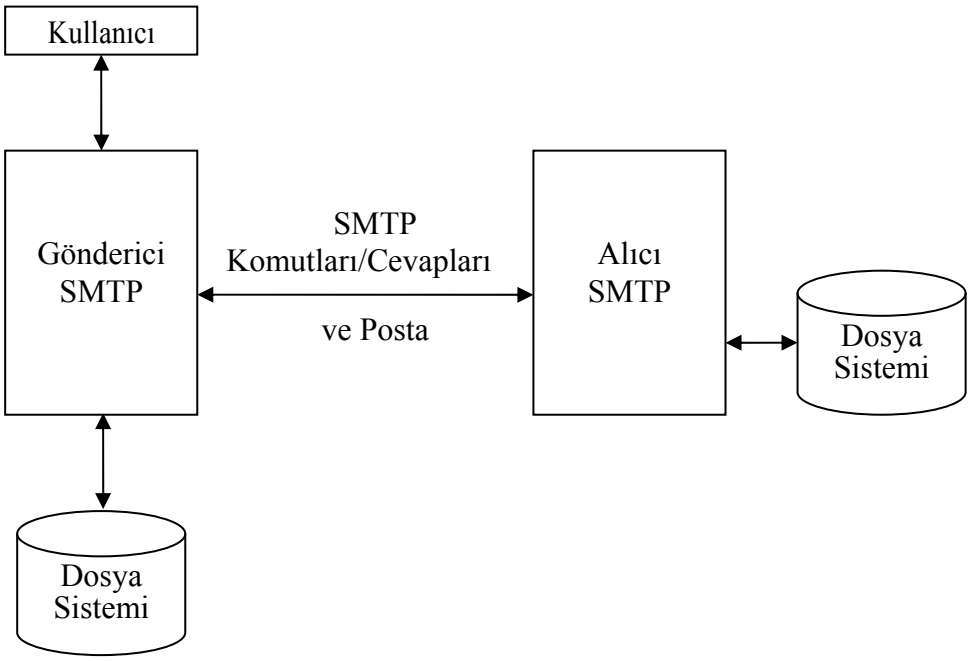
SMTP, İnternet Protokol yığınında bulunan uygulama katmanı protokollerinin en yaygın kullanıma sahip olan standartlarından biridir. RFC 821 standardı ile 1982 yılında oluşturulmuş, 1989, 1994, 1995 ve 2001 yıllarında çeşitli düzenlemelerden geçmiştir.[5] Amacı, iki kullanıcı arasındaki e-posta aktarımının verimli ve güvenli bir şekilde yapılmasıdır.

2.2.1 SMTP Modeli

Şekil 3'te SMTP'nin genel bir modeli gösterilmiştir. SMTP göndericisinin iletilmek üzere bir e-postası olduğunda, bir SMTP alıcısına iki yönlü bir aktarım kanalı kurar. SMTP göndericisinin sorumluluğu, e-postaları bir veya daha fazla sayıda SMTP alıcısına

aktarmak ve eğer varsa hataları raporlamaktır. SMTP komutları, gönderici SMTP tarafından alıcı SMTP sunucuya gönderilir ve alıcı SMTP bu komutlara SMTP cevaplarını gönderir.[1]

İşlemler gönderici SMTP'nin alıcı SMTP ile haberleşme kurması ile başlar. E-posta'nın iletilmesinden önce, iki SMTP varlığı şifrelerini veya diğer yetki işaretlerini birbirlerine ulaştırmalıdırlar. Bundan sonra gönderici, kimliğini ve e-posta alışverişi için gerekli diğer bilgileri içeren MAIL komutunu iletir. Alıcı bundan sonra MAIL komutuna bir onay geri döndürmelidir. SMTP'de, bu onay 250, veya bazı dokümanlarda 250 OK şeklindedir. Onay, istenilen e-posta aksiyonunun tamamlandığı anlamındadır.[1]



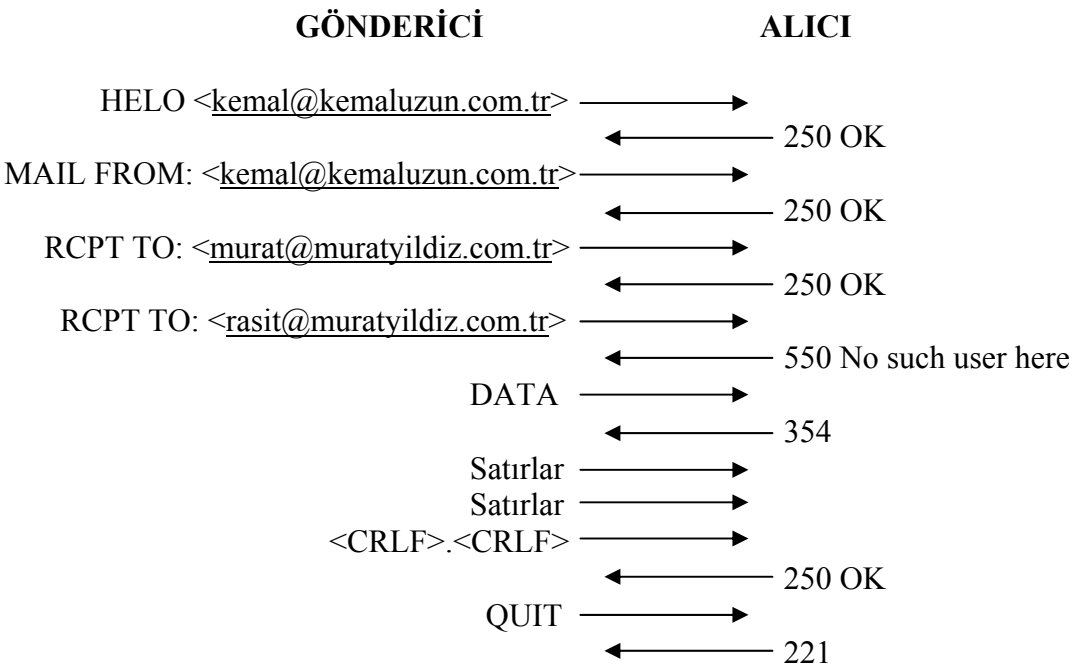
Şekil 3 – SMTP Modeli [1]

İşlemin sıradaki adımı bir RCPT komutunun iletilmesidir. Amacı mesajın hedeflerini belirtmektir. Burada da, her potansiyel alıcıdan bir onay beklenmektedir.

İşlemin üçüncü adımı DATA komutu yayınlamaktır. Bu komut gönderici tarafından yayınlanarak, alıcıya/alıcılara mesajın gelmeye hazır olduğu uyarısının yapılmasını sağlar. Veri bundan sonra; gönderici, mesajın sonunu belirten özel bir kontrol karakterleri katarı gönderene kadar, hattan hata iletilir. Özel katar gelince, sunucu bir QUIT komutu ile işlemi sonlandırır.[1]

Gönderici-SMTP kendi gönderici adres ve alıcı adres alanı için kemal@kemaluzun.com.tr şeklinde standart bir format kullanır. Burada gönderici adı kemal, alan adı tanımlayıcısı ise kemaluzun.com.tr dir.

Örnek olarak Şekil 4'de iki SMTP kullanıcısının basit bir e-posta alışverişi işlemi gösterilmiştir. Şeklin sol tarafında göndericinin bağlantı kurması gösterilmiştir. HELO komutu iki makine arasında bir bağlantı kurulması için tanımlayıcı alışverişi olarak kullanılmıştır. MAIL FROM komutu muratyildiz.com.tr alan adı için yeni bir e-posta geçişinin başlıyor olduğunu söyler. Alıcı bu komutu tamponlarını temizlemek, konum tablolarını resetlemek, ve mesaja hazırlanmak için kullanır. Bundan sonra, RCPT komutu alıcının ileri yol adresini verir, örneğimizde bu murat@muratyildiz.com.tr ve rasit@muratyildiz.com.tr adresleridir. murat@muratyildiz.com.tr 250 OK cevabı ile kabul edilmiş ancak rasit@muratyildiz.com.tr adresi alıcı sunucusunda olmadığından 550 cevabı ile reddedilmiştir. DATA komutu alıcıya, kendisini mesaj içeriğinin takip edeceğini bildirir. Cevap 354'tür. 354, e-posta girişini başlat ve bunu CRLF CRLF komutu ile sonlandır anlamındadır.[1]



Şekil 4 - SMTP E-Posta Transferi [1]

Veri iletilir ve iletimin sonu CRLF CRLF ile işaretlenir. Alıcı 250 OK ile cevaplar ve bağlantı QUIT ve 221 cevabı ile kesilir. Bu da sunucunun bağlantıyı kapattığı anlamına gelir. [1]

2.3. DNS (Domain Name System)

İnternette bulunan her nesnenin, etkileşime giren her sunucu ve ucun bir İnternet adresi olması gerekir. Bu adres protokol seviyesinin IPv4 ve IPv6 olmasına göre 32 bit ya da 128 bit uzunluğundadır. Alan Adı bu 32 ya da 128 bit uzunluğundaki sayı yerine insanların anlayabileceği, aklında tutabileceği, kurumsal kimlik ve marka ile özdeşleştirebileceği isimlerin kullanılmasını sağlar.[7] DNS sunucuları, İnternet adreslerinin IP adresi karşılığını kayıtlı tutmaktadır. DNS, 1983 yılında RFC 882 ve RFC 883 standartlarıyla oluşturulmuş, daha sonra RFC 1034 ve RFC 1035 standartlarıyla güncellenmiştir.[7]

DNS sistemi isim sunucuları ve çözümleyicilerinden oluşur. Bir DNS istemci, bir bilgisayarın ismine karşılık gelen IP adresini bulmak istediği zaman isim sunucuya başvurur. İsim sunucu, yani DNS sunucu da eğer kendi veritabanında öyle bir isim varsa, bu isme karşılık gelen IP adresini istemciye gönderir. DNS veritabanına kayıtların elle, tek tek girilmesi gerekir. Bir alan hakkında bilgi bulunduran, alanının MX (Mail eXchanger), NS (Name Server) ve A (Address) kayıtlarının tutulduğu sunucular ise Yetkili İsim Sunucuları'dır.

Çözümleme(Resolving) ise iki şekilde yapılır; özyineli çözümleme ve özyineli olmayan çözümleme. Bir sorgu özyineli ise, doğrudan sorulan adrese karşilik gelen IP adresi ya da "makina bulunamadı" cevabı verilebilir. Fakat özyineli olmayan(yinelemeli) bir sorguda cevabı bulmak için başka bir isim sunucusunun IP'si verilebilir. [7]

3. SPAM E-POSTA SİSTEMİ

3.1. SPAM Nedir?

E-posta ve SMTP, İnternet'in ilk hizmetlerinden birisi olmasından dolayı şu anda İnternet hizmetleri söz konusu olduğunda önemle ihtiyaç duyulan güvenlik, hız, kimlik kontrolü gibi gereklilikler göz önünde bulundurulmamıştır. Bu yüzden e-posta altyapısı günümüzde İnternet'in önemli problemlerine zemin oluşturmaktadır. Hemen hemen her e-posta kullanıcısı her gün posta kutusunda istemediği birçok reklam vb. amaçlı e-posta ile karşılaşmaktadır.

SPAM, kişilere veya kurumlara kendi rızaları olmadan, onların hem zamanlarını alacak hem de sistem kaynaklarını boşa harcatacak istek dışı e-posta gönderilmesidir. SPAM, aslında kelime olarak Amerikan kökenli bir kelime olup, 1960'lı yıllarda Geo. A. Hormel and Company şirketi tarafından üretilen baharatlı domuz eti ve jambon konservesinin adıdır. "Spiced Pork and Ham" kelimelerinin kısaltmasından oluşmaktadır. 1970 yılında İngiltere televizyonunun ünlü komedi programı Monty Phyton'da, işlenmiş gıda yemek istemeyen bir çiftin bir lokantanın menüsünde SPAM içeren ürünlerden başka birşey bulamayıp bu ürünü yemek zorunda kalmaları konu edilmişti. O tarihte çok popüler olan bu skeçten ilham alınarak istenmeyen reklam amaçlı e-postalara da SPAM adı verilmeye başlanmıştır.[19] SPAM çoğunlukla ticari reklam niteliğinde olup, bu reklamlar sıklıkla güvenilmeyen ürünlerin, çabuk zengin olma kampanyalarının duyurulması amacına yöneliktir. SPAM gönderici açısından çok küçük bir harcama ile gerçekleştirilebilirken mali yük büyük ölçüde e-postanın alıcıları veya taşıyıcı servis sağlayıcı kurumlar tarafından karşılanmak zorunda kalınır.[8]

İlk SPAM girişimi, 1 Mayıs 1978 tarihinde DEC'in ABD'nin batı kıyısındaki tüm ARPANet adreslerine yaptığı ürün tanıtımı olarak kabul edilmektedir:

Mail-from: DEC-MARLBORO
rcvd at 3-May-78 0955-PDT
Date: 1 May 1978 1233-EDT
From: THUERK at DEC-MARLBORO
Subject: ADRIAN@SRI-KL
DIGITAL WILL BE GIVING A PRODUCT PRESENTATION OF THE NEWEST MEMBERS OF THE

DECSYSTEM-20 FAMILY; THE DECSYSTEM-2020, 2020T, 2060, AND 2060T. THE DECSYSTEM-20 FAMILY OF COMPUTERS HAS EVOLVED FROM THE TENEX OPERATING SYSTEM
AND THE DECSYSTEM-10 <PDP-10> COMPUTER ARCHITECTURE. BOTH THE DECSYSTEM-2060T
AND 2020T OFFER FULL ARPANET SUPPORT UNDER THE TOPS-20 OPERATING SYSTEM.
THE DECSYSTEM-2060 IS AN UPWARD EXTENSION OF THE CURRENT DECSYSTEM 2040 AND
2050 FAMILY. THE DECSYSTEM-2020 IS A NEW LOW END MEMBER OF THE DECSYSTEM-20
FAMILY AND FULLY SOFTWARE COMPATIBLE WITH ALL OF THE OTHER DECSYSTEM-20 MODELS.
WE INVITE YOU TO COME SEE THE 2020 AND HEAR ABOUT THE DECSYSTEM-20 FAMILY AT
THE TWO PRODUCT PRESENTATIONS WE WILL BE GIVING IN CALIFORNIA THIS MONTH.
THE LOCATIONS WILL BE:
TUESDAY, MAY 9, 1978 - 2 PM
HYATT HOUSE (NEAR THE L.A. AIRPORT)
LOS ANGELES, CA
THURSDAY, MAY 11, 1978 - 2 PM
DUNFEY'S ROYAL COACH
SAN MATEO, CA
A 2020 WILL BE THERE FOR YOU TO VIEW. ALSO TERMINALS ON-LINE TO OTHER
DECSYSTEM-20 SYSTEMS THROUGH THE ARPANET. IF YOU ARE UNABLE TO ATTEND, PLEASE
FEEL FREE TO CONTACT THE NEAREST DEC OFFICE FOR MORE INFORMATION ABOUT THE
EXCITING DECSYSTEM-20 FAMILY.

O günden bu yana SPAM çoğunlukla ürün ya da hizmet pazarlamak gibi ticari amaçlara hizmet etmiştir. [9]

3.2. SPAM E-posta Nasıl Anlaşılır?

SPAM e-postalar genel olarak ilk bakışta Gönderen ve Konu satırlarıyla normal e-postalardan ayırt edilebilmektedir. Ancak SPAM göndericilerin gün geçtikçe farklı yöntemler kullanmalarıyla birlikte, günümüzde hiç alakası olmayan bir kurumdan veya arkadaşımızdan gelmiş gibi görünen SPAM e-postalarla karşılaşmaktayız. SPAM e-postaların ayırt edici tipik özellikleri aşağıdaki şekilde özetlenebilir.

- Birden fazla alıcıya aynı içerik ile gönderilirler.
- Genel olarak tanıtım amacıyla gönderilirler.
- Genellikle içerikleri yalan ya da yanıltıcıdır ve alıcıya hiçbir şey ifade etmezler.
- Dini inanç ya da insani duyguları konu edebilirler ve e-postanın belli bir sayıda kişiye iletilmesini isteyebilirler.
- Gönderen, Kime gibi adres bilgileri uygun biçimde değildir ve genellikle rastgele sahteleri üretildiğinden harf hatalarına oldukça sık rastlanır.
- E-posta mesaj başlık bilgileri tahrip edilmiş olur ve bu sebeple geriye dönük izleme zor olur.
- Alıcıların bu dağıtımdan e-posta almak istemediklerini belirtebilecekleri geçerli veya fonksiyonel bir geri dönüş adresi bulunmaz.

Şekil 5'te SPAM e-postaların Konu kısmında sıklıkla kullanılan ifadeler verilmiştir. Burada göründüğü gibi 2007 yılında Konu kısmında Re: ve boş olarak gönderilen SPAM e-postalar yüzde 10 gibi önemli bir orana ulaşmıştır. 2008 yılında ise Konu kısmında en çok kullanılan ifade oranının yüzde 0.4 te kalması, Konu kısmında kullanılan ifadelerin sürekli değişen bir grafik izlediğini göstermektedir.

İnternette alışveriş yapmak gün geçtikçe daha popüler bir duruma geldiği için, SPAM göndericiler kullanıcıların ilgisini çekmek amacıyla sipariş durumu ile ilgili konuları kullanmaktadırlar. [10]

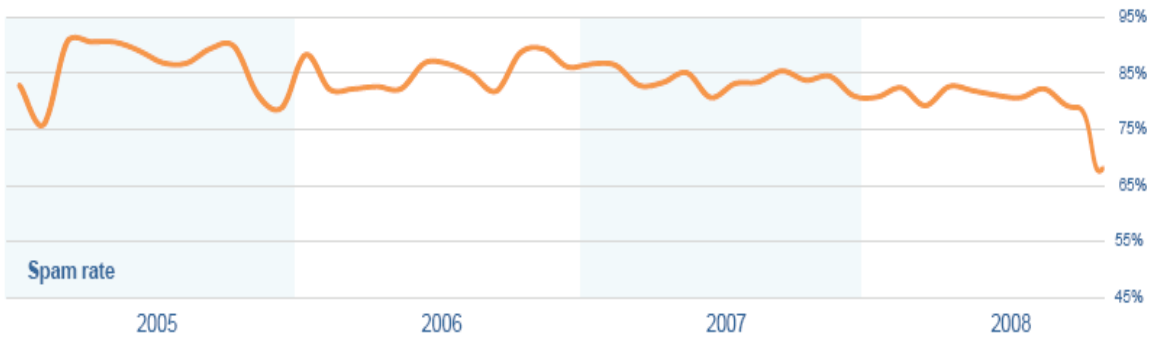
2007 Subject Lines	%	2008 Subject Lines	%
Re:	7.18%	Your order	0.43%
<empty subject line>	2.78%	Re: Order status	0.41%
The Pharmacy America Trusts	2.12%	RE: Message	0.41%
The United States National Medical Association	1.47%	Replica Watches	0.41%
Fw:	1.47%	Re:	0.38%
Replica Watches	1.12%	Free porno DVD's to download	0.23%
Man Lebt nur einmal - probiers aus !	0.97%	Downloadable porno DVD's for free	0.23%
Can you tell me what's wrong, and how we can fix it?	0.96%	Exquisite Replica	0.22%
You've received an ecard from a Partner!	0.85%	CNN Alerts: My Custom Alert	0.18%
You've received a greeting ecard from a Worshipper!	0.81%	Hi	0.16%

Şekil 5 – SPAM E-Postalarda Konu Kısmında Kullanılan İfadeler [10]

3.3. SPAM E-Posta Trafiği

E-posta, haberleşme amacıyla kullanımının artması ve yalınlığı sayesinde, suiistimal edilmek için uygun bir araç haline gelmiştir. Dünya çapındaki e-posta trafiğinin ortalama yüzde 85'lik bölümünü SPAM e-postalar oluşturmaktadır.

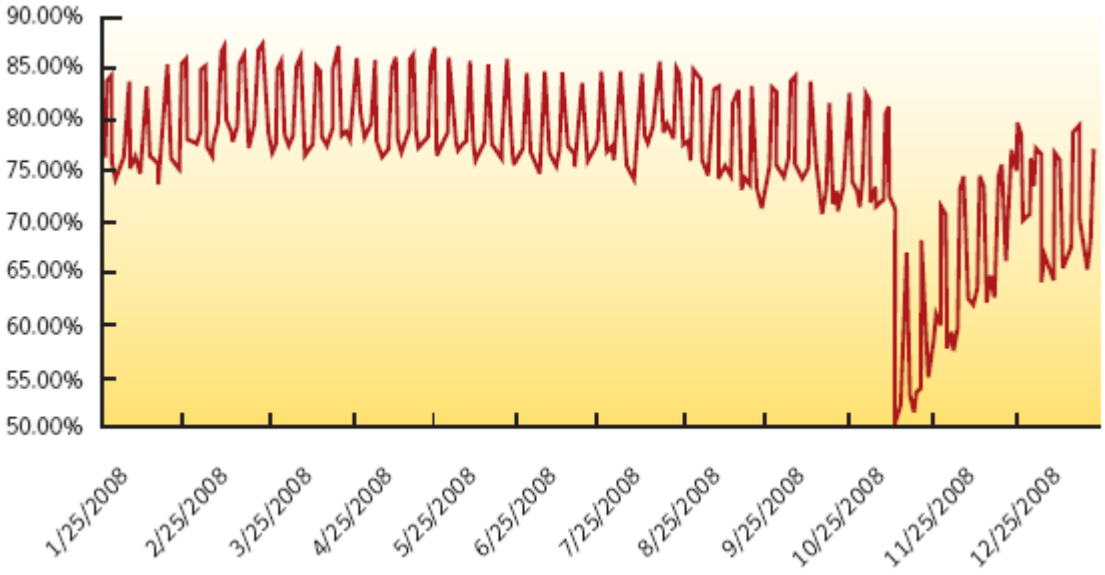
Şekil 6'da SPAM e-postaların yoğunlukları yıllık olarak verilmiştir. SPAM e-posta yoğunluğunun 2005 yılından 2008 yılı sonlarına kadar ortalama yüzde 80 ile yüzde 90 aralığında seyrettiği görülmektedir.



Şekil 6 - Yıllara Göre SPAM E-Posta Yoğunlukları [11]

2007 yılı için genel SPAM e-posta yoğunluğu yüzde 84,6 olmuşken, 2008 yılı için genel SPAM e-posta yoğunluğu, yıl sonundaki ani düşüş sebebiyle yüzde 81,2 oranına kadar gerilemiştir. [11]

Şekil 7'de 2008 yılına ait SPAM e-posta yoğunlukları verilmiştir. Burada 2008 yılının kasım ayında SPAM e-posta yoğunluklarında gerçekleşen ani düşüş daha detaylı bir şekilde görülmektedir.



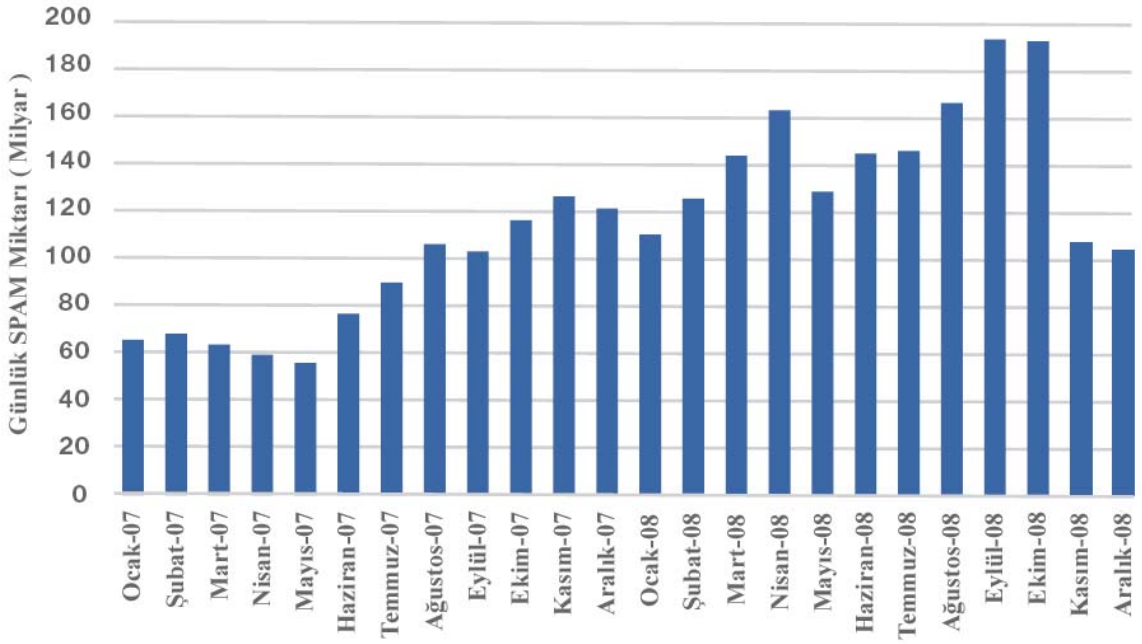
Şekil 7 - Aylara Göre SPAM E-Posta Yoğunlukları [12]

SPAM e-posta yoğunluğundaki bu ani düşüşe, 11 Kasım 2008 tarihinde Amerika Birleşik Devletleri'nin Kaliforniya eyaletinden çıkış yapan McColo sağlayısının bağlantısının kesilmesi neden olmuştur. McColo'nun barındırma hizmeti verdiği ağlarda yaklaşık 450 bin zombiye dönüşmüş bilgisayar olduğu ve bunlardan oluşan Botnet'lerin yönetilerek milyarlarca SPAM e-posta gönderimi için kullanıldığı tespit edilmiştir. Bu sebeple McColo bağlantısının kesilmesi Srizbi, Mega-D gibi önde gelen Botnet'lerin kontrolünü geçici de olsa kaybetmelerine sebep olmuştur.

11 Kasım 2008 tarihinden sonra kurulan SPAM e-posta tuzaklarında daha önceki seviyelere göre %25'lik bir azalma gözlenmiştir. Daha da önemlisi genel olarak SPAM e-postaların ana kaynağındaki değişikliklerdir. McColo Amerika dışında faaliyetlerine devam ederken McColo'nun yani SPAM e-postaların ana operatörünün kapatılmasından

sonra ülkelerin dağılımı ile ilgili olarak çok ani ve aşırı bir değişiklik gözlemlenmiştir. [10]

2007 – 2008 yıllarına ait günlük SPAM e-posta miktarlarının verildiği Şekil 8'e bakıldığında, yıl ortalaması olarak 2008 yılında dünya çapındaki SPAM e-posta miktarının 2007 yılına göre yaklaşık 2 katına çıktığı görülmektedir.

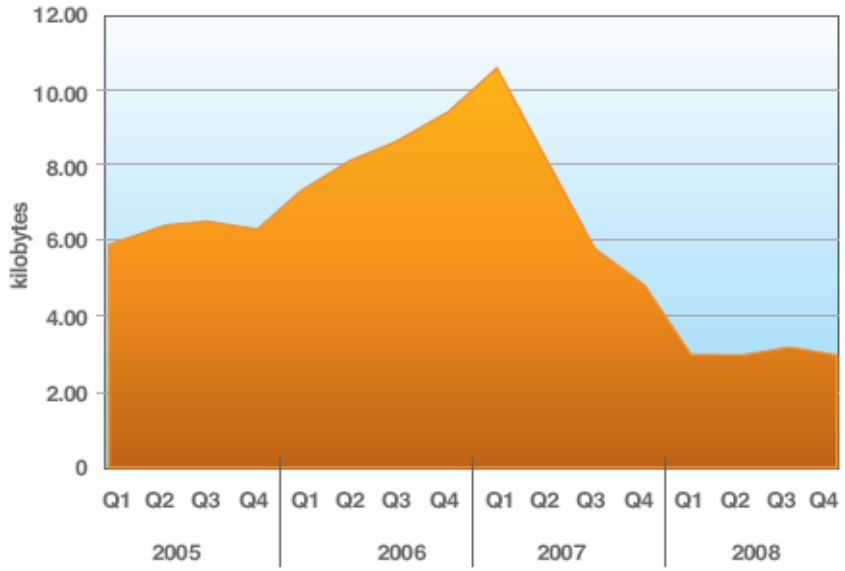


Şekil 8 - Günlük Ortalama SPAM E-posta Miktarları [13]

2007 yılının haziran ayında yükselişe geçen SPAM e-posta miktarları 2008 yılının eylül ayında en üst seviyeye çıkarak günde yaklaşık 200 milyara ulaşmıştır. Kasım ayında McColo servis sağlayısının bağlantısının kesilmesiyle günlük SPAM e-posta miktarı yaklaşık 100 milyara kadar gerilemiştir.

Şekil 9'da SPAM e-postaların 2005 – 2008 yılları arasındaki ortalama büyüklükleri verilmiştir. SPAM e-posta büyüklükleri, resim içerikli SPAM e-postalarla paralel olarak artarak, 2007 yılının ilk çeyreğinde 10 KB değerini aşarak en üst noktaya ulaşmıştır.

SPAM e-postaların ortalama büyüklüklerindeki en önemli değişiklik 2007 yılının sonunda gerçekleşmiştir. Bu değişiklik resim içerikli SPAM e-postalardaki düşüşe bağlı olarak meydana gelmiş ve ortalama 3-4 KB değerine kadar gerilemiştir. [10]



Şekil 9 – Ortalama SPAM E-Posta Büyüklükleri [10]

2008 yılında SPAM e-posta büyüklüğü az da olsa yükselme eğilimi gösterse de McColo bağlantısının kesilmesiyle düşmeye başlamıştır. [10]

SPAM e-posta gönderiminin 2008 yılına ait coğrafi dağılımı Şekil 10'da verilmiştir. Görüldüğü gibi SPAM e-posta trafiğinin önemli bir kısmını A.B.D. oluşturmaktadır.

Ülke	SPAM E-Posta Oranı
A.B.D.	15.9%
Türkiye	7.4%
Rusya	7.2%
Çin	6.1%
Brezilya	5.1%
İngiltere	3.4%
Kore	3.3%
Polonya	3.2%
Hindistan	3.0%
İtalya	3.0%
Almanya	3.0%
İspanya	2.8%
Arjantin	2.5%
Kolombiya	2.3%
Tayland	2.2%
Fransa	2.0%
Diğer	27.6%

Şekil 10 - SPAM E-postaların Ülkelere Göre Oransal Dağılımı [13]

3.4. SPAM Türleri

SPAM sadece e-posta ile sınırlı bir hareket değildir. Aşağıdaki şekillerde de karşımıza çıkabilmektedir:

- Faxlarda.
- Cep telefonlarında.
- ICQ, MSN, Jabber gibi anlık mesajlaşma servislerinde.
- Web arama motorlarında.
- USENET haber gruplarında.

İnternet veya rehberlerden öğrenilen fax numaralarına istek dışı gönderilen reklam veya teklifleri de SPAM kapsamında değerlendirmek mümkündür. Aynı şekilde alışveriş yapılan yerlerin ya da bankaların cep telefonlarına gönderdikleri tanıtım ve bilgilendirme mesajları da SPAM olarak ele alınmaktadır.

Web arama motorlarına yönelik SPAM'ın en bilinen yöntemi "Google Bombing" dir. Kendi içerisinde bir "rank" (puanlama) sistemini barındıran Google, bu sistemin kötü amaçlı kullanımı sonucu amaç dışı bir işlev yerine getirmektedir. Basitçe bir koddan oluşan robot yazılım farklı sistemleri kullanarak Google'a aynı kelimeyi defalarca aratmakta ve çıkan sonuçlar arasından kendi kayıtlarında bulunan sayfaya yönlenmektedir. Bu sayede yönlenilen sayfanın "rank" i yükselmekte ve böylece sonuç sayfasında yükseklere çıkmaktadır. Sonuç olarak belirli bir anahtar kelime sonucunda sadece bu yöntemi kullanarak kendi sırasını yükselten sayfa, kullanıcıların daha çok giriş yaptığı bir sayfa olmaktadır.[5]

Bir diğer SPAM türü de USENET mesajları aracılığı ile yapılmaktadır. Bu tür SPAM, sıklıkla haber öbeklerini okuyan ancak çok ender veya hiç gönderi yapmadıklarından e-posta adresleri elde edilemeyen kullanıcı grubunu hedefler. USENET SPAM'ları haber öbeklerini reklamlar veya ilgisiz iletilerle doldurarak kullanıcı açısından faydasız ve kullanılması zor hale getirir. [8]

E-posta aracılığıyla gönderilen SPAM doğrudan gönderilen mesajlarla, bireysel kullanıcıları hedef alır. E-posta SPAM listeleri genellikle USENET gönderilerinin

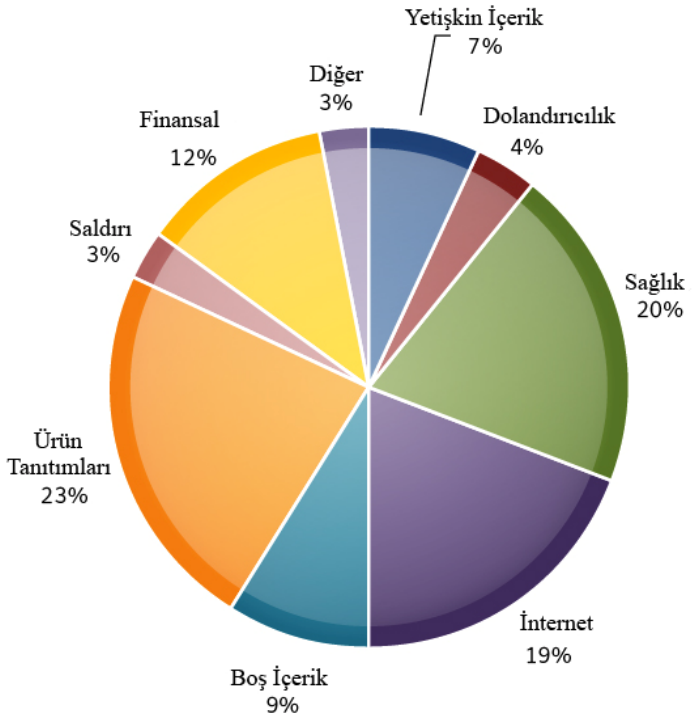
taranması, tartışma gruplarının üye listelerinin çalınması veya web üzerinden adres aramalarıyla oluşturulur. E-posta tipindeki SPAM gönderileri tipik olarak alan kullanıcının masraf yapmasına sebep olur. E-posta erişimi için süreye veya kotaya bağlı olarak her kullanıcı için bir bedel ortaya çıkması kaçınılmazdır. Ayrıca, SPAM e-postaların taşınmasının servis sağlayıcılar ve diğer online servisler üzerinde oluşturduğu mali yük de büyük ölçüde abonelere yansıyacaktır.[8]

Talep Edilmemiş Ticari E-posta (UCE – Unsolicited Commercial e-mail)**,** e-posta yolu ile gönderilen SPAM türlerindendir ve adından da anlaşılacağı gibi istemediği halde gönderilen, bir ürünü ya da hizmeti tanıtıcı e-postalardır. [8]

Talep Edilmemiş Kitlesel E-posta (UBE - Unsolicited Bulk e-mail -), içeriğinin mutlaka ticari olması gerekmeyen, aynı anda yüz binlerce kişiye gönderilen e-postalardır. Bu e-postalar ticari içerikli olabileceği gibi politik bir görüşün propagandasını yapmak yada bir konu hakkında kamuoyu oluşturmak amacı ile gönderilen e-postalar da olabilir. Herkesin üzerinde hemfikir olduğu, önemli bir toplumsal duyarlılığa sahip bir konu hakkında görüş bildirmek için kitlesel olarak gönderilen bir e-posta da SPAM olarak nitelendirilebilir. [8]

Kolay Para Kazanın (MMF - Make Money Fast) e-postaları, zincir e-postalar ya da piramit benzeri pazarlama yapıları ile ilgili gelen e-postalardır. Piramitin en üstündeki isme para gönderip listenin altına kendinizi eklediğinizde para kazanmaya başlayacağınıza ilişkin e-postalar bu türe örnek olarak verilebilir. [8]

SPAM e-postalar içeriklerine göre sınıflandırıldığında sağlık ve ürün tanıtımlarıyla ilgili e-postalar ön plana çıkmaktadır. Şekil 11'de görüldüğü gibi sağlık, İnternet ve ürün tanıtımlarıyla ilgili SPAM e-postalar genel olarak tüm SPAM e-postaların çoğunluğunu oluşturmaktadır.



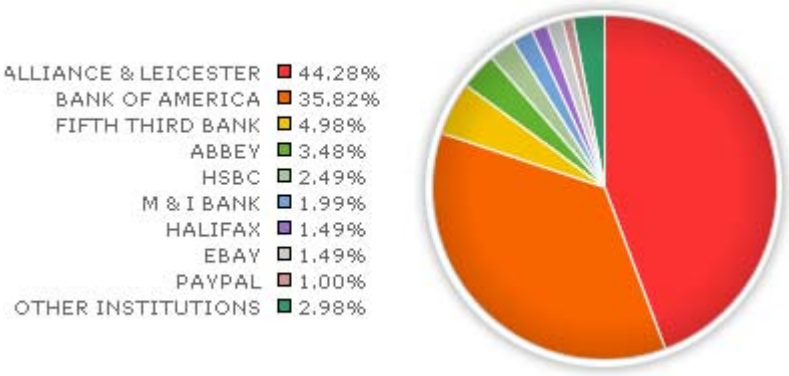
Şekil 11 - SPAM E-postaların İçeriklerine Göre Oransal Dağılımları [12]

Son zamanlarda buradaki Yetişkin İçerik kategorisi altındaki arkadaşlık ve flört SPAM e-postaları son derece popüler olmuştur. İçerik olarak Dolandırıcılık kapsamında yer alan Phishing yöntemi, her ne kadar oransal olarak düşük gibi görünse de verdiği zararlar bakımından ayrıca ele alınmalıdır.

3.4.1. "Phishing"

Phishing son yıllarda ortaya çıkmış ve SPAM şeklindeki gönderimlerle yayılan bir tuzak sistemidir ve sonuçları SPAM e-postaya göre oldukça ağır olmaktadır. Phishing tekniğinde SPAM e-postada olduğu gibi toplu bir e-posta listesine bir e-posta gönderilmektedir. Teknik olarak SPAM e-posta şeklinde olsa da içerik olarak birbirinden ayrılır.[5] Phishing'de e-posta içeriği alıcıyı yanlış ve ilgi çekici ibarelerle saldırganın sitesine yönlendirerek daha çok kimlik bilgilerini doğrulama amacına yöneliktir. Phishing genellikle banka veya ebay gibi alışveriş sitelerinin taklit edilmesiyle, resmi/yasal e-posta izlenimi vererek, e-posta alıcısından siteye giriş bilgilerinin teyidini isterler. Alıcı da e-postayı gerçek zannettiği için siteye yönlenir ve giriş bilgilerini girer. Böylece saldırgan tarafından kontrol edilen bir web sitesine bu bilgiler girilmiş olur ve saldırganlar bu bilgilerle istedikleri işlemi yapabilirler. [14]

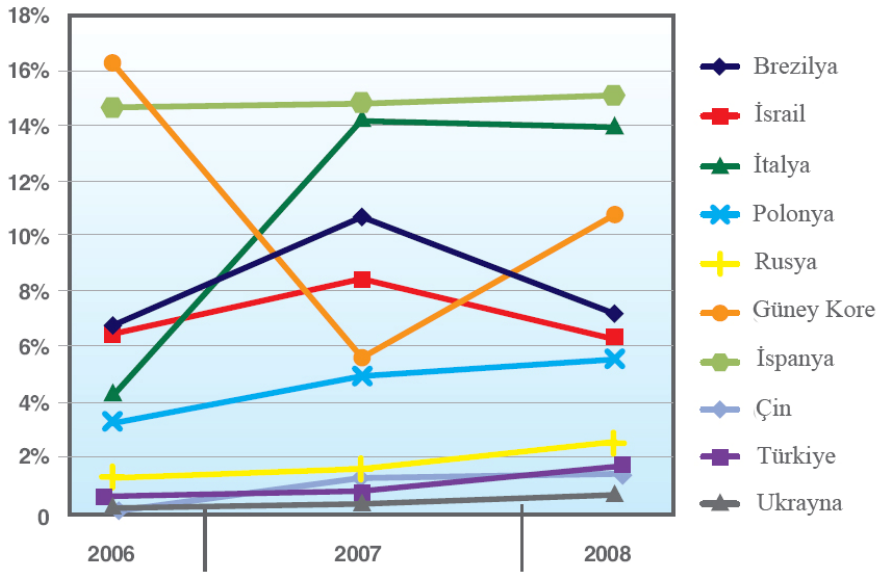
Veri güvenliği şirketi Marshal tarafından yayınlanan haftalık raporda Phishing yöntemiyle taklit edilen kurumlar Şekil 12'de yer almaktadır. Göründüğü gibi taklit edilen kurumların hemen hepsi banka ve alışveriş sitelerinden oluşmaktadır.



Şekil 12 – Phishing Yönteminde Taklit Edilen Kurumların Oransal Dağılımları [15]

Örnek olarak vermek gerekirse, ülkede yaygın biçimde tanınan bir banka tarafından gönderilmiş gibi gelen bir e-posta, banka hesabınıza bir hesaptan yüklü miktarda havale yapıldığını ve bu havaleyi onaylamak için belirtilen yere İnternet bankacılığı kodunuz ve şifrenizi girmeniz gerektiğini, tıpkı ilgili bankadan gönderilmiş gibi gelir. Eğer alıcı bu tuzağa düşer ve belirtilen yere istenen bilgileri yazarsa, saldırgana bilgilerini kendi elleri ile vermiş olur. Bundan sonra saldırgan aldığı bilgilerle alıcının hesabından kendi paravan hesaplarına para aktarır.[5]

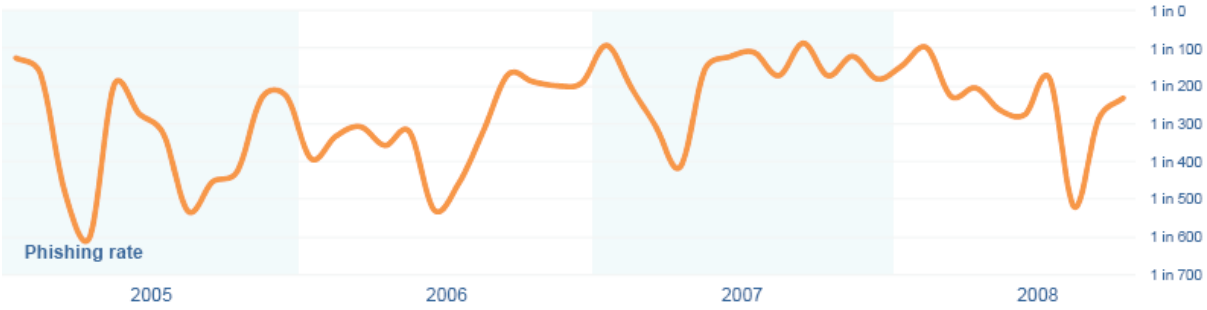
Şekil 13, Phishing türündeki SPAM e-postaların ülke bazında dağılımını göstermektedir.



Şekil 13 - Phishing E-postaların Ülke Bazında Oransal Dağılımı [10]

Son üç yıl ortalamasında İspanya yüzde 15 oranıyla üst noktada yer almışken, İtalya ve Kore de Phishing trafiğinin önemli bir bölümünü oluşturmuştur. Brezilya ve İsrail ise her ne kadar 2008 yılında düşme eğilimi gösterse de halen önemli Phishing e-posta kaynaklarındandır.

Yıllık dönemler halinde Phishing trafiği Şekil 14'de verilmiştir. Her ne kadar inişli çıkışlı bir grafik izlese de ortalama olarak 2006 yılında yükselişe geçen Phishing, 2007 yılında yüzde 0,6 oranına ulaşarak ortalama her 156 e-postadan birinde saptanmıştır. 2008 yılına gelindiğinde şubat ayında en üst noktasına çıkarak yaklaşık yüzde 1 oranıyla 99 e-postadan biri Phishing olmuştur. 2008 yılı ortalamasına bakıldığında ise bir azalma olmuş ve yüzde 0,4 oranına düşerek ortalama her 244 e-postadan birinin Phishing olduğu tespit edilmiştir. Bu düşüşün en önemli sebebi, aynı dönemde tüm SPAM e-posta trafiğinin düşüş sebebi olarak da kabul edilen 2008 yılının son çeyreğinde McColo sağlayıcısının kapatılmasıdır. Bu durum aynı zamanda Phishing e-postaları için de özel Botnetlerin kullanılmaya başlandığının bir göstergesidir. [11]



Şekil 14 - Phishing E-Postaların Tüm E-Posta Trafiği İçindeki Yeri [11]

2008 yılında Phishing içerikli SPAM e-posta göndericileri gerek finansal kriz gerekse banka müşterilerindeki belirsizlik unsurlarını kullanmışlardır.[10]

Bir diğer önemli konu ise Phishing yönteminde kullanılan web siteleridir. APWG (Anti Phishing Work Group) tarafından Kasım 2005 de yayımlanan bildiride değinildiği üzere Phishing yapılırken kullanılan sahte sitelerin ortalama 5,5 gün çevrimiçi kalmakta ve sonra kendilerini yok etmektedir. Bu sürenin kısıtlı olması, mağdurların hukuki süreçte saldırganın izini bulmakta güçlük çekmelerine sebep olmaktadır. Çünkü saldırgan ortalama beş buçuk günde kılık değiştirmektedir. [5]

3.5. SPAM E-postanın Hukuksal Durumu

Ülkemizde bilişim suçu kavramı Türk Ceza Hukukuna ilk defa 1991 yılında 3756 sayılı Kanunla girmiş olup "Bilişim Alanında Suçlar" başlığı altında Türk Ceza Kanunu'nun 525 inci maddesinin (a-b-c-d) bentlerinde düzenlemeler yapılmıştır.[16]

Bu kanundan sonra bilişim alanında günümüze kadar birçok yasal düzenleme yapılmış ve son olarak 2007 yılında Emniyet Müdürlüğü bünyesinde "Bilişim Suçları ve Sistemleri Şube Müdürlüğü" kurularak yine aynı yıl içerisinde 5651 no'lu "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" yürürlüğe girmiştir. [17] Ancak bunca düzenlemeye rağmen SPAM e-posta gönderimi konusunda açık bir ifadeyle herhangi bir yasal düzenleme yer almamıştır. Bu sebeple SPAM e-postalar içerik ve verdikleri zararlara göre bazı yasalarla değerlendirilmektedir. SPAM e-posta gönderimi;

- TCK md. 136: Verileri Hukuka Aykırı Olarak Ele Geçirme
- Tüketicinin Korunması KHK md. 16
- 556 sayılı Markaların Korunması KHK
- TK Kişisel Bilgilerin İşl. Yön: md. 20- İstek Dışı Haberleşmeler

maddelerine konu olurken, phishing içerikli SPAM e-postaların yaptırımı;

- TCK md. 136: Verileri Hukuka Aykırı Olarak Ele Geçirme
- TCK md. 243: Bilişim Sistemine Girme
- TCK md. 158: Nitelikli Dolandırıcılık

maddeleriyle uygulanabilmektedir.[18]

Amerika Birleşik Devletleri 2003 yılında yürürlülüğe giren ve halk arasında anti-SPAM kanunu olarak bilinen "CAN-SPAM Act" (Controlling the Assault of Non-Solicited Pornography and Marketing) yasası dahilinde SPAM ve bağlantılı olan alt sorunlarla savaşta hukuki dayanak yaratmıştır. CAN-SPAM kanunu yürürlülüğe girdiği 2003 yılından itibaren başta Microsoft olmak üzere birçok firma tarafından yasaya dayanarak SPAM davaları açılmıştır.[5] Amerika Birleşik Devletleri, daha yıkıcı olan phishing

içerikli SPAM e-posta göndericileri için de 2005 yılında "Anti-Phishing Act" yasasını, 250 bin USD'a kadar para ve 5 yıla kadar hapis cezası yaptırımlarıyla yürürlüğe koymuştur. [18]

Avrupa Birliği ise "2000/31/EC sayılı Elektronik Ticaret Direktifi" ve "2002/58/EC sayılı Gizlilik ve Elektronik Haberleşmeler Hakkında AB Direktifi" yasalarıyla SPAM e-postalarla mücadele etmektedir.[18]

3.6. SPAM E-Posta Adres Kaynakları

SPAM göndericilerinin, SPAM e-postaları göndermek için öncelikle e-posta adreslerini içeren bir listeye ihtiyaçları vardır. Bir SPAM gönderici ne kadar çok e-posta adresine sahipse o kadar çok müşteri potansiyeli var demektir. Bu nedenle e-posta adreslerini toplayan ve dosyalayan şirketler aracılığıyla, alınıp satılan ticari bir değer haline de dönüşmüştür. Hatta el altından yüz binlerce e-posta adresinin depolandığı CD'ler satılmakta olup, bunların reklamları da yine SPAM e-postalarla yapılmaktadır.[19] SPAM göndericiler de e-posta adreslerini kendileri toplayabildiği gibi bu tip şirketlerden de tedarik edebilmektedirler.

E-posta adreslerini ele geçirmenin çeşitli yolları vardır. Ancak çoğu zaman bu adresler, adres sahiplerinin kendileri tarafından bilinçsizce SPAM göndericilere ulaştırılmaktadır: [19]

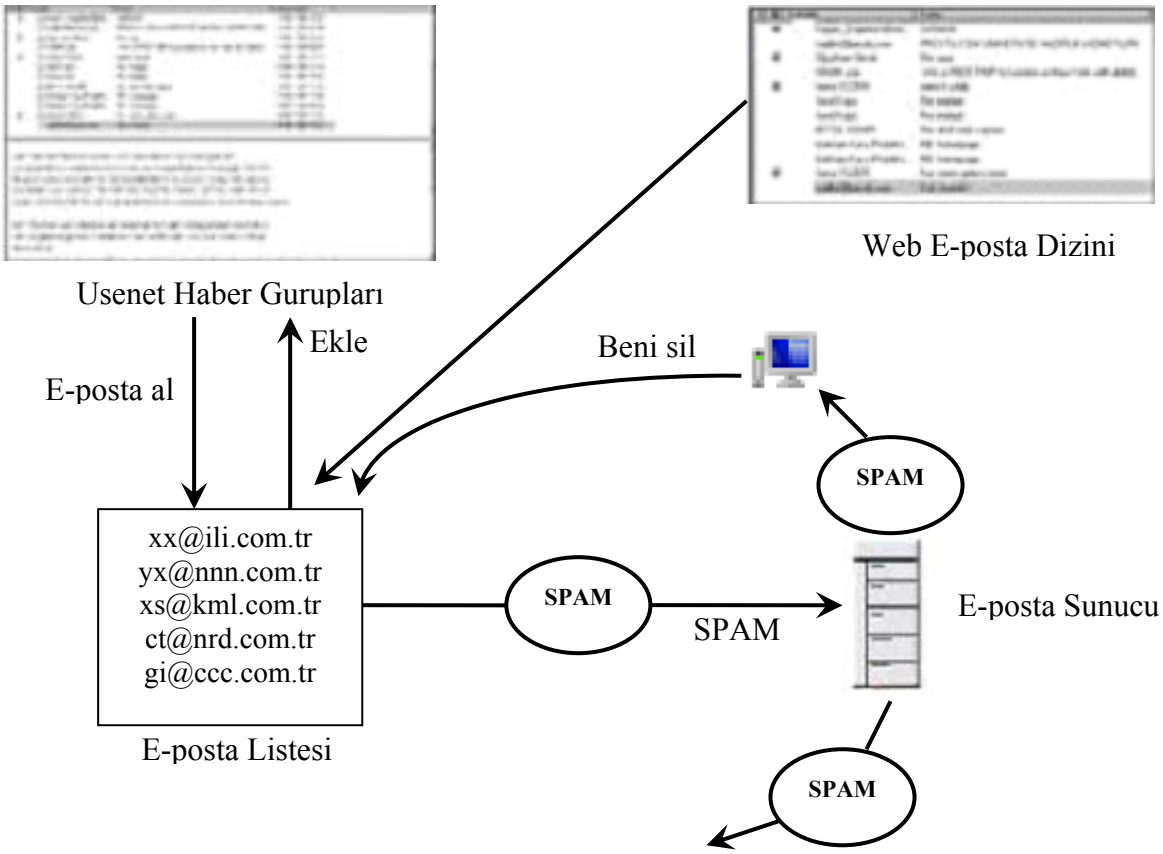
a) "Bedava Üyelik" gerektiren siteler
b) E-Posta yönlendirmeleri (Forwarding)
c) Web siteleri
d) Sözlük Saldırısı (Dictionary Attack)
e) Bilgisayar virüsleri
f) Geri Bildirim

a) "Bedava Üyelik" gerektiren siteler: Şarkı sözü sitelerinden forumlara kadar birçok site, kullanımının ücretsiz olduğunu, ancak sadece e-posta adresi ile üyelik gerektiğini söylerler. Eğer site, özel olarak aldığı e-posta adresini kimseye vermeyeceğini ve SPAM

amaçlı olarak kullanmayacağını açıkça ifade etmiyorsa büyük bir ihtimalle bu adres bir veritabanında SPAM göndericilere satılmak üzere depolanacaktır. Hatta bazı siteler bunu açıkça yazsalar dahi kullanıcılardan topladıkları adresleri SPAM amaçlı olarak kullanmaktadırlar. [19]

b) E-Posta yönlendirmeleri (Forwarding): Bazen bir tanıdıktan gelen fıkra, resim gibi içeriklerle gelen e-postalar, büyük bir beğeniyle alan kullanıcı tarafından hemen kendi tanıdıklarına yönlendirilir. Yönlendirirken e-postanın içinde daha önceki göndericilerin de e-posta adresleri birikir. Sonunda biriken bu e-posta adresleri bir SPAM göndericinin eline geçer. Bu, alıcıların herhangi birinin bilgisayarında bulunan bir casus yazılım ile olabileceği gibi, alıcının kendisi SPAM göndericilere para karşılığında adres satan bir kişi bile olabilir. Bazı e-postalar özellikle kullanıcıların duygularını sömürecek şekilde hazırlanır. Çok popüler bir ürünün aslında kanserojen olması, milli ve manevi değerlere hakaret içeren web sitelerini protesto etmek için oy kullanılması, aslında hiç olmayan kanserli bir kıza yardım istekleri, şans getireceğine inandırılan e-postalar buna örnek olarak verilebilir. [19]

c) Web siteleri: Dünyadaki Web sitelerini dolaşıp veri toplayan robot yazılımlar mevcuttur. Bunlar, USENET haber guruplarını, web sayfalarını ve web üzerinden dolaşan mesaj içeriklerini tarayarak bütün mesajların içindeki e-posta adreslerini bulmaya çalışırlar. En çok yakalamaya çalıştıkları karakter "@" işaretidir. Bu nedenle bazı sitelerde e-posta adresleri, "xx (at) xyz.com" şeklinde yazılırlar ki bu tür robotlara daha az takılsın.[19] Ayrıca bu yazılımlar chat alanlarına, örneğin America Online'a girip e-posta adresi toplayabildikleri gibi tartışma listelerine üye olarak ta bu tür işlemleri gerçekleştirebilirler. [20]



Şekil 15 – SPAM Web [20]

d) Sözlük Saldırısı (Dictionary Attack): SPAM göndericiler, sözlük saldırısı yöntemiyle rastgele e-posta adresleri üreterek bu adreslere e-posta göndermektedirler. Özellikle çok kullanılan isimleri bazen alfabetik, bazen ters alfabetik bazen de rastgele seçilmiş isimler şeklinde RCPT komutuyla deneyerek alıcı adreslerinin saptanması şeklinde gelişen SMTP aktarımlarıdır.[21] Genellikle büyük şirketler bu tip saldırıların hedefi haline gelirler. Çünkü SPAM göndericiler açısından, çok sayıda kullanıcısı olan alan adlarında bir ismin bulunabilme şansı bir kaç kullanıcısı olanlardan daha yüksektir.

e) Bilgisayar virüsleri: Kullanıcının bilgisayarına giren ve bu amaçla tasarlanmış virüsler, kullanıcının haberi olmadan e-posta programının (Outlook vb.) adres defterindeki ve hatta birikmiş tüm e-postalardaki adresleri toplayıp yine İnternet üzerinden SPAM göndericilere ulaştırabilmektedir.[19]

f) Geri Bildirim: Bazı SPAM göndericiler mesajlarında SPAM e-posta listesinden çıkmak isteyenler için bir geri dönüş adresi bulundururlar. Daha fazla SPAM e-posta almak

istemeyen kişiler bu adrese bir mesaj gönderirler ve otomatik olarak listeden çıkarılırlar. Fakat SPAM göndericiler genelde bunun olmasına izin vermedikleri gibi artık bu durumu e-posta adreslerinin doğruluğunu tespit için kullanır hale gelmişlerdir. [20]

3.7. SPAM E-Posta Gönderme Teknikleri

SPAM e-postalar, içerik ve gönderme teknikleri açısından geçmişten günümüze gelişerek devam etmiştir:

3.7.1. Standart E-posta

İlk SPAM, e-posta adresine doğrudan, bir e-posta sağlayıcısı aracılığı ile kişisel adreslerle gönderme şeklinde ortaya çıkmıştır. Bu şekilde gönderilen bir SPAM e-postayı engellemek de bir o kadar kolaydı çünkü gönderen kişinin adresini bloke etmek sorunu çözmekteydi. Bu şekilde gerçekleşen bloke etmeler SPAM göndericileri yeni arayışlara itmeye etken olmuştur.

3.7.2. Dial-Up ve ADSL Bağlantısı

SPAM göndericiler 1990'lı yıllarda Dial-Up (çevirmeli ağ) bağlantısını kullanarak SPAM göndermeye başlamışlardır. Burada servis sağlayıcısı kendi kullanıcılarından aldığı e-postaları farklı kullanıcılara yollamaktadır. SPAM göndericiler de, dinamik Dial-Up bağlantısı sayesinde, daha önce engellenmiş olsalar dahi her seferinde farklı IP adreslerinden SPAM gönderme imkânı bulmuşlardır. Bunun üzerine servis sağlayıcıları, kullanıcılarına belli kotalar getirmeye başlayarak, Dial-Up bağlantılarının listesi tutup bunları da bloke edilmeye başlamışlardır.

2000'li yılların başında ADSL kullanımının artmasıyla SPAM göndericiler, bu bağlantının da dinamik türünü kullandıkları gibi, kullanıcı sistemlerindeki açıkları da kullanmaya başlamışlardır. Birçok ADSL modeme kontrolsüz ve parolasız erişim sağlayarak ADSL kullanıcıları üzerinden SPAM e-posta göndermeye başlamışlardır.

3.7.3. SPAM Kamuflajı

E-posta mesajlarında teknik olarak yollayanın adını ve adresini gerçek dışı olarak her şekilde göstermek mümkündür. Örneğin ilk bakışta gönderen kişi olarak sizin ad ve adresinizin görüldüğü bir e-posta, herhangi bir başka kişiye sizin veya bağlı bulunduğunuz kurumun hiç ilgisi olmadan gönderilebilir. Gerçek e-posta adreslerini saklamak amacıyla, e-posta başlığındaki Kime, Gönderen, Yanıtla bölgelerinin sahtelerini üretebilirler. Böylece e-posta, SPAM gönderici değil de, başka birinden geliyormuş gibi görünür. Buna "SPAM Kamuflajı" da denebilir.[20]

E-postanın başlık kısmının detayları özel olarak incelenip gönderildiği IP adresi bulunabilse dahi, SPAM göndericiler kendileriyle ilişkisi olmayan Open Relay sunucu veya sunucularla, milyonlarca e-postayı toplu bir şekilde gönderebilmektedirler. Bunların tespiti de pratikte çok daha zor olabilir. Bu nedenle SPAM gönderici, satılan ürün hakkında daha çok bilgi alınabilmesi için bir geri dönüş adresi, bir web sitesi ya da bir telefon numarası verebileceği gibi, isterse de gerçek kimliğini ve yerini kolayca gizleyebilmektedir.

3.7.4. "Open Relay"

E-posta sunucusu üzerinden herkesin herhangi bir kısıtlama olmaksızın, istediği yerden başka bir yere e-posta gönderebilmesidir.

1980'lerde sanal olarak her SMTP sunucusu birer Open Relay'dı ve e-postaları çoğunlukla tüm sunucular kabul etmekte ve e-postaları yerlerine göndermekteydiler.[21]

SPAM göndericiler, günümüzde halen Relay'a açık olan sunucuları bularak, özellikle kimliklerini gizlemek, çoğunlukla da milyonlarca e-postayı gönderirken yükü dağıtmak amacıyla kullanmaktadırlar. Bir sunucu Open Relay ise ve SPAM göndericiler tarafından kullanılıyorsa, belli başlı DNS kara listelerine uzunca bir süre kalmak üzere kaydedilebilir. Artık normal e-postalar çoğunlukla, özellikle doğrudan gönderici uçtaki bir e-posta aktarımcısı tarafından gönderilmekte ve alıcının alan adı için tahsis edilmiş e-posta alıcıları tarafından kabul edilmektedir.[21]

3.7.5. Dolaylı SPAM E-posta

Gönderici adresi taklit edilerek bir e-postaya yanıt gibi gönderilen otomatikleştirilmiş e-postalardır. Dolaylı SPAM e-posta, virüs tarama raporları ("Virüs bulundu"), bir e-postanın geçici veya kalıcı bir sorundan dolayı teslim edilemediği ve/veya bir süre daha bu teslimatın gerçekleştirilmesinin denenip denenmeyeceği hakkında e-posta göndericisine bilgi vermek için gönderilebilir.[21]

3.7.6. Sözlük Saldırısı (Dictionary Attack)

SPAM göndericiler, her ne kadar bu yöntemi e-posta adreslerini ele geçirmek için kullanıyor olsalar da, oluşan e-posta trafiği açısından SPAM e-posta ile eşdeğer yoğunluktadır. Daha önce de belirtildiği gibi bu yöntemle, rastgele e-posta adresleri üreterek bu adreslere e-posta göndermektedirler. Bu adreslerin doğru olup olmadığını tespit etmek için değişik yöntemler kullanılmaktadır. Buna örnek olarak gönderilen e-posta içerisinde bulunan resimler ekranda göründüğünde ona ilişkin URL adresi çağırıldığından, o resmi çağıran e-postanın adresini doğrulamak için yeterli olabilmektedir.

3.7.7. SPAM E-posta Gönderme Yazılımları

SPAM göndericilerin, toplu e-posta adres listelerini kullanarak, çok kısa sürede büyük miktarlardaki e-postayı teslim etmek üzere kullandıkları yazılımlardır. Bu yazılımların bir çoğunda düz metin (TXT) tabanlı veya resim içerikli (HTML) gönderim içeriği mevcuttur. Bu yazılımlar, en iyi senaryo altında mümkün olduğunca sadece e-posta teslimatı için gerekli olan SMTP istemci koduyla işbirliğine girer. Alıcı sunucularla yaptıkları SMTP diyalogunda yanlış veya belli belirsiz bilgi verirler. Komutları göndermek için alıcının yanıtını beklemezler ve eğer alıcı taraftan birkaç saniye içinde bir yanıt alamazlarsa, bağlantıyı keserler. Geçici hataların oluşması durumunda işlem yineleme mekanizmasını kullanmazlar.[21]

Genel olarak gönderme şekillerinde iki farklı yapı mevcuttur:

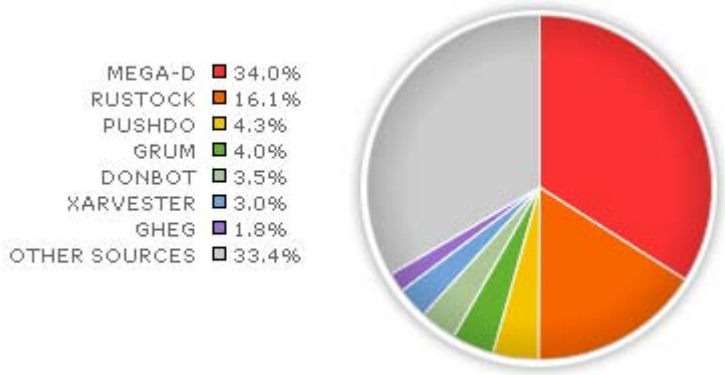
Hotmail, gmail gibi herhangi bir mail adresi üzerinden de gönderim yapılabilen DNS yapısında, günlük gönderimlerde bir sınırlama bulunmaz. Gönderim adetleri doğrudan doğruya İnternet bağlantı hızıyla ilgilidir. Bu yapıda SMTP sunucusu görevini yazılımda oluşturulmuş olan sanal bir sunucu üstlenmektedir. DNS yapısında, bir sunucuya bağlı kalınmadığından ve sınırsız sayıda SPAM e-posta gönderilebildiğinden, gönderilen e-postaların bazıları karşı tarafın SPAM e-posta adreslerine düşebilmekte ve bazı e-posta sunucuları tarafından engellenebilmektedir. Yazılımın çok sayıda bilgisayara yüklenerek SPAM e-posta gönderilmesi, gönderim sayısını oldukça arttırabilmektedir.

Diğer gönderim şekli ise, SMTP sunucularına bağlı gönderim seçeneğidir. Gönderim hızı büyük ölçüde kullanılan SMTP sunuculara bağlıdır. Gönderilecek SPAM e-posta sayısında ise yine bir sınır yoktur ancak gönderim yapılmak için seçilen SMTP sunucusu güvenli ise, sunucunun belirlediği kotalar dahilinde gönderim yapılabilir. Bu gibi detaylarında düşüldüğü bu yazılımlarda SMTP modüllerine bekletme özelliği de eklenmiştir. Bu sayede gönderimi yapılan e-postalar topluca sunucuya iletilmek yerine belirlenen zaman aralıkları ile sunucuya ulaştırılabilmektedir.

3.7.8. Botnet

Günümüzde SPAM e-posta göndermek, kullanıcı sistemlerine giren veya bulaşan yazılımlar/virüsler yardımıyla bir hayli kolaylaşmıştır. SPAM e-postalarda süren artışın, e-posta göndermek için milyonlarca ev bilgisayarını, sahiplerinin haberi olmadan kullanabilen ve "Bot" olarak da adlandırılan yazılımlardan kaynaklandığı belirtilmektedir. Bu yazılımların yüklü olduğu bilgisayar "Zombi", Zombilerden oluşan ağ ise "Botnet" olarak adlandırılmaktadır. Bilgisayar sistemlerinin belirli açıklarını kullanan bu yazılımlar, bu açıklara sahip olan bilgisayarları bulup yerleşerek, yöneticisinden gelecek görevleri beklemeye başlamaktadır. Zombiler değişmez bir şekilde Microsoft® Windows® ailesinden bir işletim sistemi kullanan bilgisayarlardır ve hemen hemen tümü mahalli IP adres bloklarındadırlar. Zombiye dönüşen bilgisayar kullanıcıları, bilgisayarlarına bu yazılımların/virüslerin bulaştığından ya haberleri yoktur ya da kendilerine zararsız göründüğü için önemsememektedirler. Çoğunlukla bu mahalli IP adres sahiplerinin servis sağlayıcıları, bunlara hizmet vermemek gibi bir önleme başvurmamaktadırlar. Bu sebeple, bu tip "mahalli" adres bloklarını veritabanlarına

ekleyen bazı DNS kara listeleri mevcuttur. Bu servis sağlayıcılardan hizmet alanlar, normal e-postalarını göndermek için bu servis sağlayıcının e-posta sunucusunu kullandıklarından dolayı, mahalli adreslerden gelen e-postaları reddetmek için bu kara listeleri kullanabilmektedirler.[21]

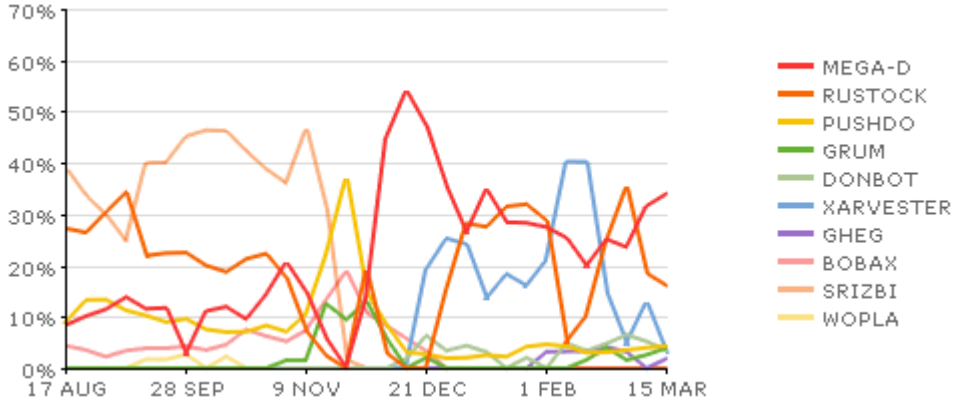


Şekil 16 – Botnet aracılığıyla gönderilen SPAM E-posta Dağılımları [43]

Şekil 16, Botnetler aracılığıyla gönderilen SPAM e-postaların Botnet'lere göre yüzdesel dağılımı göstermektedir. Tipik olarak ana botnetler SPAM gönderimlerinin tamamından sorumludur. [43] Mega-D ve Rustock Botnetleri tüm SPAM e-posta gönderimin yarısını oluşturmaktadır.

Botneti yöneten kişiler bu ağı, SPAM e-posta göndermek, herhangi bir hedefe saldırmak, kimlik, kredi kartı..vb kişisel bilgileri toplamak veya farklı yazılımlar yüklemek için de kullanabilmektedirler. SPAM göndericiler, kendileri Botnet oluşturabilecekleri gibi, Botnet sahibi kişilerden bu ağı kiralayarak kendi amaçları için kullanabilmektedirler. Botnet sayesinde, milyonlarca SPAM e-postayı çok kısa bir sürede göndermeleri mümkün olabilmektedir.

Şekil 17'de Botnet kaynaklı alınan SPAM e-postaların 2008-2009 dönemine ait geçmişi gösterilmektedir.



Şekil 17 – Dönemsel Botnet kaynaklı SPAM E-Posta Faaliyetleri [43]

11 Kasım 2008 tarihinde McColo sağlayıcısının bağlantısının kesilmesiyle botnet kaynaklı milyarlarca SPAM e-postanın önüne geçilmiştir. Şekil 17'de görüldüğü gibi Kasım ayında Srizbi başta olmak üzere birçok Botnet kaynaklı SPAM e-postalarda önemli düşüşler görülmektedir. Belli başlı Botnetlerin büyüklükleri ve faaliyetleri kısaca aşağıdaki gibidir.

3.7.8.1. Botnet ve Storm

100.000 zombiden oluşmaktadır. Yeniden tasarlanan otomatik e-posta ve DNS sistemi ile Şifreli haberleşme ve iletişim sağlar. 2009 yılının Şubat ayındaki Windows güncellemelerinden dolayı faaliyetlerinde aksama olmuştur.[11]

3.7.8.2. Botnet ve Srizbi

1.300.000 zombiden oluşmaktadır. Tüm SPAM e-postaların yüzde 50'sinden sorumludur. SPAM e-postalar kutlama, sahte link ve sahte video siteleri dahil olmak üzere sahte haber başlıklıdır. Kernel modundaki SMTP bileşeni, yerel güvenlik duvarlarından saklanabilen, özel TCP kümesiyle Windows güvenliğini devreden çıkarabilen, çok hızlı ve ölçeklenebilir bir yapıdadır. Kasım ayında McColo'nun bağlantısının kesilmesiyle birlikte faaliyeti yüzde 60 oranında azalmıştır.[11]

3.7.8.3. Botnet Cutwail

1.000.000 zombiden oluşmaktadır. Tüm SPAM e-postaların yüzde 25'inden sorumludur. Genellikle erkeklik geliştirici ürünler, aldatıcı sahte tebrik kartları ve kötü amaçlı propaganda linklerinden oluşur.[11]

3.7.8.4 Botnet ve Mega-D

150.000 zombiden oluşmaktadır. Emir ve komutaya bağlı olarak faaliyet gösterir. Kasım ayında Mccolo'nun bağlantısının kesilmesiyle faaliyeti yüzde 80 oranında azalmıştır.[11]

3.7.8.5. Botnet ve ASPROX

100.000 zombiden oluşmaktadır. Özellikle SQL enjekte saldırılarını yönetmek için tasarlanmıştır. Art niyetli java scriptler aracılığıyla web sitelerinin bozulmasıyla, esas olarak Phishing amacıyla kullanılır. Kasım ayında Mccolo'nun bağlantısının kesilmesiyle faaliyeti yüzde 80 oranında azalmıştır.[11]

3.7.8.6. Botnet ve Rustock

90.000 zombiden oluşmaktadır. Buradaki bazı SPAM göndericiler Srizbideki kaynakları paylaşabilirler. İşlemleri gizlemek amacıyla Kernel modunda çalışan kök bileşenleri ve şifrelenmiş emir komuta bileşenlerini kullanırlar. SPAM e-postalar kutlama, sahte link ve sahte video siteleri dahil olmak üzere sahte haber başlıklıdır. Kasım ayında McColo'nun bağlantısının kesilmesinden dolayı faaliyeti yüzde 50 oranında azalmıştır. [11]

3.7.8.7. Botnet ve Warezov

50.000 zombiden oluşmaktadır. Rastgele gibi görünen alan adları kullanılır. Toplu SPAM e-posta ve webmail SPAM göndermek için kullanılır. Kasım ayında McColo'nun bağlantısının kesilmesiyle faaliyetleri önemli ölçüde aksamıştır.[11]

3.7.8.8. Botnet ve Gheg

500.000 zombiden oluşmaktadır. Parfümeri ürünleriyle ilgili ve Fransızca SPAM e-posta göndermek için kullanılır.[11]

3.8. Resim İçerikli SPAM E-posta

Geçen yıllar içerisinde içerik filtrelemesinde istatistiksel yöntemlerin kullanımı metin içerikli SPAM e-postalar ile mücadelede oldukça başarılı bir grafik sergilemiştir. Ancak bu yöntemler geliştirilirken SPAM göndericileri de bu yöntemleri atlatmak için yeni yöntemler geliştirmiştir. [22] E-posta mesajın sonuna ya da ortasına, text bütünlüğü içinde bir kesinti ile kelimeleri bozarak veya fon renginde rastgele seçilmiş bir harf, kelime veya cümle koyarak, anti-SPAM yazılımlarını yanıltmaya çalışarak gelişen yöntemler, günümüzde resim tabanlı SPAM e-postalarıyla en uç noktaya ulaşmıştır.

Resim içerikli SPAM e-postalar basit resim işleme tekniklerini kullanmakta olup bu teknikler her bir e-postanın içeriğine göre değişiklik göstermektedir. Örneğin arka plan renklerinin değiştirilmesi, font türleri veya resimlere yapay doku eklenmesi gibi. Bu sebeplerle geleneksel metin tabanlı içerik ile çalışan SPAM filtreleme yazılımları tarafından farkedilmezler. [23]

Şekil 18'de 2008 – 2009 dönemine ait resim içerikli SPAM e-postaların tüm SPAM e-postalar içerisindeki yüzdesini göstermektedir.

Şekil 18 – Resim İçerikli SPAM E-Posta Trafiği [43]

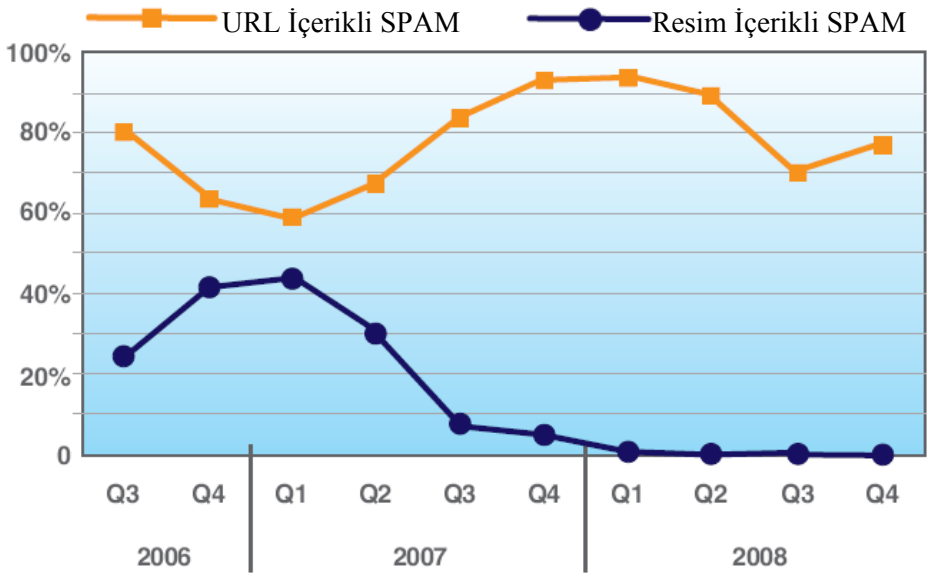
Eylül 2008'de yükselmeye başlayan Ekim ayında yüzde 10 seviyesine ulaştıktan sonra Kasım ayından itibaren hızlı bir düşüşle yüzde 1 seviyesine kadar gerilemiştir. URL içerili SPAM e-posta konusunda verilmiş olan Şekil 19'da görüleceği gibi geçmiş dönemlerde resim içerikli SPAM e-postalar sürekli artarak 2007 yılının ilk çeyreğine yüzde 40 oranını aşmıştır. Bu tarihten sonra URL içerikli SPAM e-postaların popüler olmasıyla resim içerikli SPAM e-postalar sürekli azalarak yüzde 1 seviyesine kadar gerilemiştir.

Resim içerikli olarak iletilen veri, metin tabanlı SPAM e-postalarına oranla çok daha fazla bant genişliği ve disk alanı kullanımına yol açmaktadır. Bu sebeple SPAM göndericilerin mevcut kaynaklarıyla daha fazla SPAM e-posta gönderebilmek için resim içerikli SPAM e-posta gönderiminden vazgeçtiklerini düşünmek mümkündür.

3.9. URL İçerikli SPAM E-posta

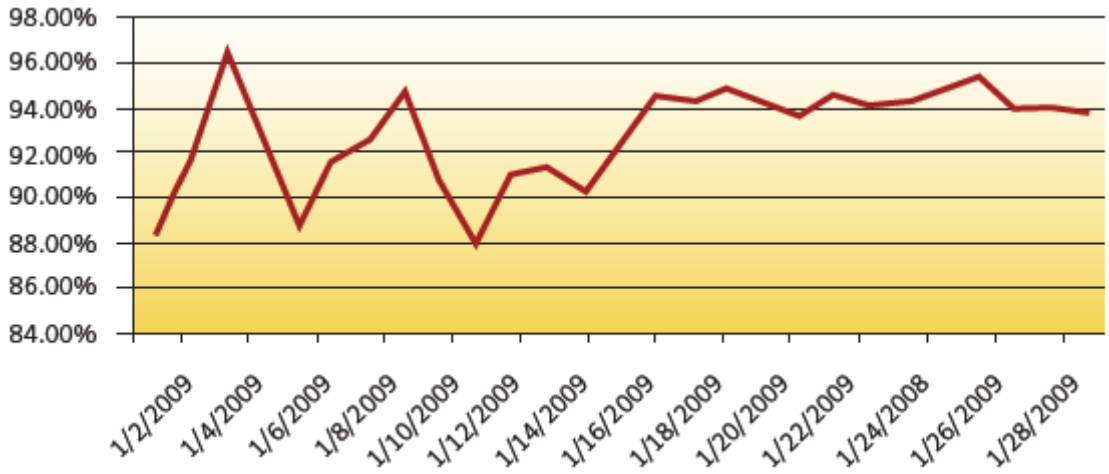
SPAM e-posta ile alıcıya bir URL linki ulaştırılır ve linkin tıklanmasıyla birlikte iletilmek istenen SPAM içeriğin yer aldığı web sitelerine yönlenilir.

2007 yılında resim içerikli SPAM e-postalardaki azalma eğilimi 2008 yılında da sürekli bir biçimde devam etmiştir. SPAM göndericiler bu tip SPAM e-postalar yerine URL içerikli SPAM e-postalar göndermeyi tercih etmişlerdir.[10]



Şekil 19 – URL ve Resim İçerikli SPAM E-Posta Dağılımları [10]

Şekil 19'da URL içerikli SPAM e-postalardaki artış gösterilmekte olup resim içerikli SPAM e-postalarda tam tersi bir yönde azalma olduğu görülmektedir. [10] 2008 yılının son çeyreğinde yükselişe geçen URL içerikli SPAM e-postalar Şekil 20'de görüldüğü gibi 2009 yılının ilk ayında yüzde 95 seviyesine kadar ulaşmıştır.



Şekil 20 – Ocak 2009 URL İçerikli SPAM E-Posta yoğunlukları [12]

URL içerikli SPAM e-posta sürekli arttığından bu e-postalarda kullanılan alan adlarına bakmak gerekir. Aşağıda birbirini takip eden Şekil 20 ve Şekil 21'de 2008 yılında en çok kullanılan 10 alan adı gösterilmiştir.

Rank	January 2008	February 2008	March 2008	April 2008	May 2008	June 2008
1.	googlepages.com	blogspot.com	blogspot.com	crazeben.com	doubleclick.net	dogpile.com
2.	sarahkverok.com	81.222.138.69	powref.com	manninst.com	livefilestore.com	kewww.com.cn
3.	magnarx.com	goldsmallman.com	nuelig.com	hyuaien.com	maddris.com	ynnsuue.com
4.	nesoeteaok.com	fastmansilver.com	gelsedde.com	pobueitah.com	nubteku.com	wpoellk.com
5.	lifefreeart.com	dotoneauto.com	mewlegos.com	congratym.com	moieiaus.com	movecontinent.com
6.	sgmykrtrewt.com	dedeiooss.com	findmilk.com	timeminute.com	coridez.net	moptesoft.com
7.	qualiveok.com	geocities.com	marketthen.com	camethank.com	zimpleq.com	varygas.com
8.	nightboylost.com	hotripefruit.com	seatbar.com	wroteleast.com	mislie.com	earexcept.com
9.	northmanestimate.com	topstopcool.com	believeagree.com	writecotton.com	pogieamdo.com	fullrow.com
10.	geocities.com	fastpetsilver.com	somelisten.com	saveany.com	poskeij.com	colonytop.com

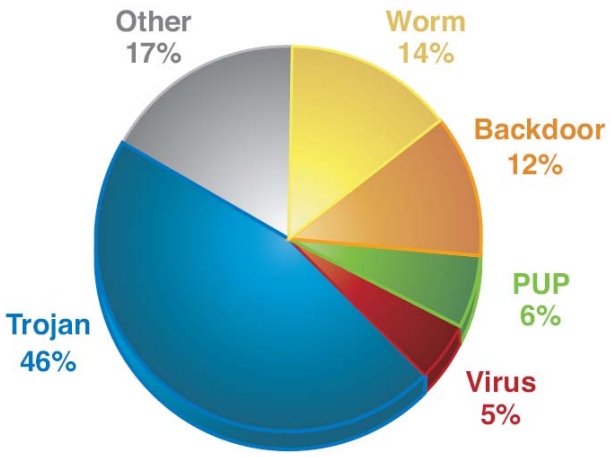
Şekil 20 - URL SPAM E-postalar içerisinde En Çok Bilinen Alan Adları, 2008 H1 [10]

Rank	July 2008	August 2008	September 2008	October 2008	November 2008	December 2008
1.	livefilestore.com	cnn.net	livefilestore.com	livefilestore.com	live.com	gucci.com
2.	smellshort.com	cnn.com	imageshack.us	live.com	tubdyqwenqe.com	notdune.com
3.	elementdepend.com	msn.com	beroyal.info	el1te-russ1an-g1rls.com	eurocasinokd.com	hereidea.com
4.	opera.com	msnbc.com	forformisskasino.com	myrusfriend.net	stop-fl0p.net	live.com
5.	grayany.com	imageshack.us	totalwrite.com	yellowpages.com	bbc.co.uk	heatdark.com
6.	creasehappiness.com	reoisk.com	cazinoyoumeyou.com	livechatfreex.com	hop-m0p.com	namenot.com
7.	msn.com	google.com	casinonewtrip.com	googlegroups.com	t1p-top.com	idolreplicas.com
8.	boceph.com	soieuu.com	csinomonster.com	cazinosostermor.com	eurocasinokg.com	davavkos.com
9.	alizedup.com	royalfirsteuro.info	beroyal.mobi	777-models-777.com	n1cewomen7.com	vutovlaf.com
10.	augsid.com	royalfirsteuro.mobi	beroyal.org	cazinomonste.com	sexymodels123.net	conemain.com

Şekil 21 - URL SPAM E-postalar içerisinde En Çok Bilinen Alan Adları, 2008 H2 [10]

3.10. Kötü Amaçlı Yazılım (Malware - Malicious Software)

Bilgisayar teknolojilerinin gelişmesi ile birlikte bilgi ve bilgisayar güvenliği konusunda en ciddi tehditlerin başında kötü amaçlı yazılımlar gelmektedir. Kötü amaçlı yazılım bulaştığı bir bilgisayar sisteminde veya ağ üzerindeki diğer makinelerde zarara yol açmak, bilgileri ve kontrolü ele geçirmek veya çalışmalarını aksatmak amacıyla hazırlanmış yazılımların genel adıdır. Bilgisayarların zombiye dönüşerek Botnetlerin oluşmasındaki en büyük etkendir. Dolayısıyla bir bakıma Botnetleri yöneten SPAM göndericilere hizmet ederek SPAM e-posta trafiğinde önemli bir rol üstlenmektedir. Şekil 22'de kötü amaçlı yazılım türlerinin 2008 yılındaki yüzdelik dağılımı verilmiştir.



Şekil 22 - Kategorilerine Göre Kötü Amaçlı Yazılım Türleri [10]

Şekil 22'de görüldüğü gibi 2008 yılında kötü amaçlı yazılımların büyük bir bölümü trojan olarak sınıflandırılmıştır. Diğer türlere genel olarak göz atılacak olursa;

• Worm: E-posta, ağ paylaşımları, çıkarılabilir sürücüler, dosya paylaşımı ya da anlık mesajlaşma uygulamalarıyla kendi başlarına yayılırlar.[10]

• Backdoor: Etkilenen sistemde, uzak bir saldırgana giriş veya çalıştırma işlevleri sağlar.[10]

• Trojan: Bilgi gözetleme ve ele geçirme gibi bir takım zararlı fonksiyonları gerçekleştirir, çeşitli bilgileri gizlice çalar ve diğer kötü amaçlı yazılımların yüklenmesini sağlar.[10]

• PUP (Potentially Unwanted Programs): Kullanıcının onayı gerekmeden yüklenen bu programlar kötü amaçlı kullanılabilir ve sistemin güvenliğini olumsuz yönde etkiler. Örn: Adware, Hacktools, Sniffers.. vs [10]

• Virüs - Bir dosya bulaşmasıyla yayılırlar. E-posta yoluyla yayılmaya başlamasıyla birlikte farklı bir boyut kazanmıştır.

3.10.1. E-posta Virüsleri

Virüsler çok uzun yıllardır bilinmekte ancak kabuk değiştirip e-posta sisteminde faaliyetlerine devam etmektedirler. 1999 yılında ortaya çıkan "Melissa" virüsü e-posta sistemi üzerinden yayılmış bilinen ilk virüstür. Melissa'dan sonra 2000 yılında ortaya çıkan LoveLetter virüsü de yine aynı şekilde e-postalar üzerinden yayılmış ve yeni bir sorunun ortaya çıkmasına öncülük etmişlerdir. Her iki virüste önceki sorunlarda olduğu gibi kullanıcıya aldatmaca içeren bir şekilde posta yoluyla gelmekte daha sonra tuzağa düşen alıcının bilgisayarına bulaşmakta ve durumu bir adım öteye götürerek mağdurun bilgisayarında bulunan tüm e-posta listesine kendisinin birer kopyasını göndermektedir. Bu sayede yayılan LoveLetter virüsünün şimdiye dek 10 milyar doların üzerinde zarara yol açtığı sanılmaktadır.[5]

4. SPAM E-POSTA ENGELLEME YÖNTEMLERİ

4.1. “Open Relay”

Bir e-posta sunucusunun açık relay olması, farklı ağ ve kullanıcıların o sunucu üzerinden izinsiz bir şekilde herhangi bir yere e-posta gönderebilmesidir. Bu sebeple açık relay sunucular SPAM göndericilerin en önemli araçları arasındadır. Bu şekilde gönderilen SPAM e-postaların direkt olarak önlenebilmesi oldukça yararlı bir yöntemdir. Bu SPAM e-postalar basit izleme teknikleri kullanılarak İnternet Servis Sağlayıcıları tarafından algılanabilmektedir. Bu trafik İnternet Servis Sağlayıcının kendi ağı içinde gerçekleştiğinden dolayı aynı zamanda e-posta faaliyetleri ile ilgili olarak periyodik bir rapor almak da mümkündür. [24] Günümüzde, özellikle e-posta sunucularını kendi bünyesinde barındıran kurumların birçoğu, farkında olmamaları ya da bu durumu önemseyecek teknik bilgiye sahip olmamaları sebebiyle e-posta sunucularını açık relay olarak kullanmaya devam etmektedirler.

Şekil 23. Relay’a Açık Durum [25]

Relay’a açık bir e-posta sunucusunun SPAM göndericilerin hedefi haline gelmesiyle birlikte e-posta sunucucunun trafiği yüksek boyutlara ulaşacaktır. SPAM göndericilerin hedefi haline gelen açık relay bir e-posta sunucunun karalistelere girmesi kaçınılmazdır, kaldı ki birçok RBL organizasyonu açık relay sunucuları, herhangibir SPAM e-posta gönderimi olmasa dahi karalistelerine almaktadırlar. Bu sebeplerden dolayı açık relay, hem SPAM e-posta gönderimini engellemek hem de oluşan SPAM trafiğinden kurtularak güvenli bir e-posta alış verişi sağlamak için mutlak suretle çözüm bulunması gereken önemli bir unsurdur. Sunucular genel olarak relay’a kapatılarak sadece yerel ağ dışında e-posta erişimi istenen kullanıcı veya ağlar için relay’a izin verilmelidir.

Şekil 24. Relay'a Kapalı Durum [25]

Bir e-posta sunucusunun relaya açık olup olmadığı, bazı organizasyonların (örn: *http://www.abuse.net/relay.html*) web sayfalarından test edilerek anlaşılabilmektedir.

Aşağıda bazı e-posta sunucuları, open relay sorunu bakımından değerlendirilmiştir. Detaylı bilgi ve diğer sucunular için *http://www.mail-abuse.com/an_sec3rdparty.html* adresine başvurulabilir.

4.1.1. Qmail

Qmail sürüm 0.91'den itibaren relay'i varsayılan olarak engellemektedir. qmail-smtpd daemon geçerli hedef adresleri ve reddedilecekleri hesaplayan rcpthosts kontrol dosyasından sorumludur.

Buradaki hassas nokta relay'in nasıl engelleneceği değil izinli host'lara relay'in nasıl açılacağı konusudur. Bu husus qmail FAQ'larında cevaplanmıştır. Burada belirli host ve ağlara relay'e nasıl izin verileceğine ait method açıklanmıştır. Russell Nelson çözümünde geçerli POP3 hesaplarına, ağlarından bağımsız olarak relay'e izin verilmesini garantilemektedir. [26]

Qmail, ücretsiz olup, Unix sistemlerde çalışmaktadır. Bilgi: *http://www.qmail.org/*

4.1.2. Sendmail Version 8

Sürüm 8.9.0'dan itibaren sendmail relay'i varsayılan olarak engellemekte olup bu özelliğin kontrolüne ilişkin birçok parametre sağlamaktadır.

Sendmail sürüm 8.8.4 e-postanın kötü amaçlı kullanılmasına karşı bazı kurallar getirmiştir. Sendmail konfigürasyonunda izinsiz relay'lere karşı check_rcpt kuralını eklemek mümkündür.

Claus Aßmann, sendmail sürüm 8'in anti-SPAM kapasitesi hakkında verdiği teknik bilgilerde, check_rcpt kuralının relay'e karşı koruma amaçlı nasıl kullanılacağını göstermiştir. Miquel van Smoorenburg ise MX'lerin listelediği alan adlarının relay'e nasıl izin verileceği hakkında bilgiler vermiştir. Diğer bir yaklaşım ise e-posta sunucusunun sadece POP hesaplarına sahip kullanıcılara izin verebilmesi şeklinde sınırlamaktır. Buna POP-önce-SMTP çözümü de denir. Uygulaması oldukça güç olmasına rağmen birçok kullanıcısı olan yerler (örneğin ISP'ler) için iyi bir çözümdür. [26]

Sendmail, ücretsiz olup, Unix sistemlerde çalışmaktadır. Bilgi: *http://www.sendmail.org/*

4.1.3. Microsoft Exchange Server

Eğer yerel SMTP kullanıcıları varsa sürüm 5.0 relay açısından saldırıya açıktır. (Sunucular relay problemi olmayan Internet ve dahili SMTP olmayan e-posta arasında geçit olarak davranırlar.) sürüm 5.5'den itibaren, izinsiz relay hazırlıkları yapılmıştır. [26]

Exchange Server, Microsoft tarafından geliştirilmiş ticari bir uygulama olup, Win/NT sistemlerde çalışmaktadır. Bilgi: *http://www.microsoft.com/products/prodref/599_ov.htm*

4.1.4. Eudora WorldMail Server

WorldMail Server version 1.0 relay açısından saldırıya açıktır. WorldMail Server'ı izinsiz relay'e karşı güvenli yapmak için Bağlantı Yönetim Merkezi (Connection Management Center) programını ücretsiz olarak indirmek mümkündür. Ulaşımı kontrol etmek için "SMTP Relay (Non-Local Only)" seçilir ve varsayılan olarak gelen "Denied Access" seçeneği off yapılır. Daha sonra relay'e izin verilecek host'lar ve ağlar listelenir. [26]

Eudora WorldMail, Qualcomm tarafından geliştirilmiş ticari bir uygulama olup, Win/NT sistemlerde çalışmaktadır. Bilgi: *http://www.eudora.com/worldmail/*

4.1.5. MMDF

MMDF'in kaynak kodunda auth.guide içinde nasıl kullanılacağı örnekleri ile açıklanmıştır. Bu konudaki teknik bilgiye SCO web adresindeki (*www.sco.com*) 104596 numaralı makaleden ulaşmak mümkündür. [26]

MMDF, ücretsiz olup, Unix sistemlerde çalışmaktadır.
Bilgi: *http://www.irvine.com/~mmdf/*

4.1.6. Post.Office

sürüm 3.1'den itibaren relay ve SPAM'e karşı koruma başlatılmıştır. "SMTP Relay Restrictions Form." altından "Restrict relay mail except as indicated below" ayarı yapıldıktan sonra sunucu üzerinden relay'e izin verilecek hosts, ağ ve alan adı bilgileri girilir.

Bilgi bölümünde yer alan web adresinden erişilebilecek belgede yapılandırmayla ilgili örneklere ulaşmak mümkündür.[26]

Post.Office, software.com tarafından geliştirilmiş ticari bir yazılım olup, Unix ve Win/NT sistemlerde çalışmaktadır.
Bilgi: *http://www.software.com/products/Post.Office/PostOffice.html*

4.1.7. Lotus Notes ve Lotus Domino

Relay'i engellemek için notes.ini dosyasına SMTPMTA_REJECT_RELAYS=1 satırını eklemek yeterlidir. [26]

Lotus Notes ve Lotus Domino, Lotus tarafından geliştirilmiş ticari bir uygulama olup, Win/NT ve OS/2 Warp sistemlerinde çalışmaktadır.

4.2. “Open Proxy”

Proxy, bir ağ hizmeti olup farklı ağ hizmetlerine dolaylı olarak bağlantı sağlamak için kullanılır. Proxy, web içeriklerinin filtrelenmesi ve güvenlik için bazı koşulların sağlanması gibi amaçlarla kullanılabilmektedir. Örneğin bir şirketin ağındaki bir sunucuya, farklı ağdaki bir müşterisi proxy aracılığıyla erişmesi mümkündür, burada sunucuya bağlantı isteği müşteri tarafından değil proxy tarafından yapılır. [27] Open Proxy ise bu bağlantı isteklerine sınırlama getirilmemiş olan ve herhangi bir yerden gelen TCP/IP bağlantı isteklerini kabul eden ve bu istekleri yönlendiren sunuculardır.

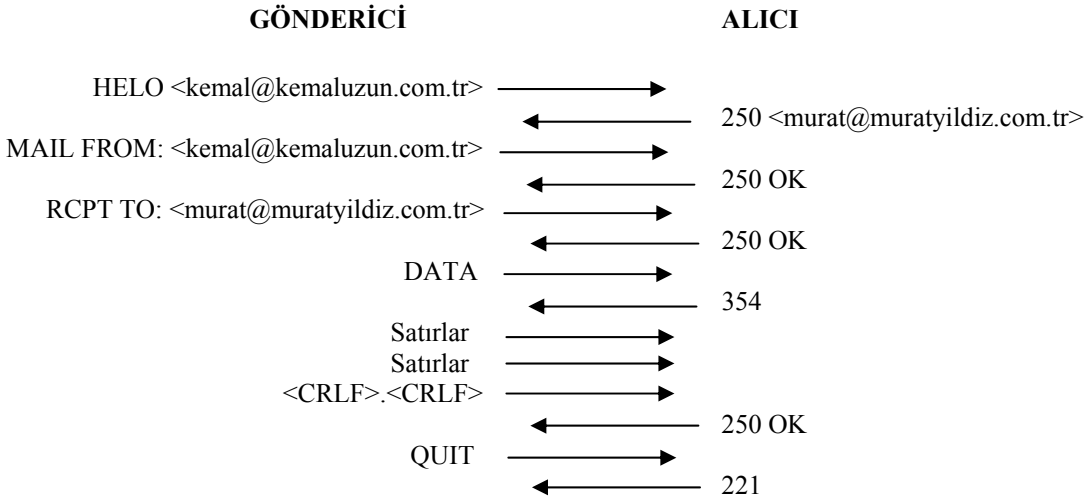
Son yıllarda open relay sunucuların giderek azalmasıyla SPAM göndericiler, IP adreslerini gizlemek ve SPAM e-posta gönderme yükünü farklı sunuculara dağıtmak için open Proxy sunucuları kullanmaya başlamışlardır.

SPAM göndericiler, bir open proxy’i kullanarak herhangi bir e-posta sunucusuna bağlanabilmekte ve o e-posta sunucusunu kullanarak SPAM e-posta gönderebilmektedir. Burada e-posta sunucusuna gelen istek proxy’den geldiği için e-posta mesaj başlığına proxy adresi eklendiğinden dolayı SPAM göndericiler için iyi bir gizlenme imkanı sağlamaktadır.[27]

4.3. Ters DNS Kaydı

Gönderilen bir e-postanın gerçek kullanıcısından gelip gelmediğini belirlemek için gelen e-postanın kaynak IP’si üzerinde yapılan DNS sorgulamasıdır. SPAM e-posta trafiğini etkin bir şekilde engelleyen ters DNS sorgulamasında, gelen e-postanın kaynak IP’sinin hangi alan adına ait olduğu belirlenir ve bu alan adının, gelen e-postadaki from adresi ile eşleşip eşleşmediği kontrol edilir. Eğer eşleşirse DNS bilgileri doğrulanmış olur ve e-posta kabul edilir. Aksi takdirde e-posta göndericisinin DNS bilgileri geçersiz kabul edilerek e-posta reddedilir.

Ters DNS sorgulaması, iki makine arasındaki SMTP aktarımının selamlaşma aşamasında gerçekleşir. SMTP aktarımı, şekil-4 de görüldüğü gibi göndericinin kendisini HELO(EHLO) komutuyla tanıtmasıyla başlar.



Şekil 4 - SMTP E-Posta Transferi

Burada alıcı tarafındaki SMTP sunucusu, ters DNS kayıt kontrolünü yapacak olan sunucudur. Gönderici kendisini, "HELO <kemal@kemaluzun.com.tr>" komutuyla, kemal@kemaluzun.com.tr olarak tanıtmıştır. Bu aşamada alıcı sunucusu, bağlantının geldiği IP adresini alarak PTR kaydını DNS'de sorgulamaktadır. Sorgulama sonucu olarak göndericinin selamlaşmada kullandığı kemaluzun.com.tr alan adı çıkarsa bağlantı kabul edilir, değilse reddedilir. Böylece, gönderici ile alıcı e-posta sunucuları arasında güvenli bir aktarım sağlanarak SPAM e-postaların engellenmesi sağlanmaktadır.
Ters DNS kaydı IP adresleri için yapıldığından dolayı bu kayıt ancak IP adreslerinin gerçek sahiplerine (ISP, Datacenter) başvurularak yada gerçek sahipleri tarafından sağlanan erişim ile yapılabilmektedir. Örneğin, 192.168.2.1 IP adresi ve *www.kemaluzun.com.tr* alan adı için kayıt yapıldığında sonuç, 1.2.168.192.in-addr.arpa PTR www.kemaluzun.com.tr şeklinde olacaktır.

Ters DNS kaydının kontrolü *http://www.dnsstuff.com* veya *www.mxtoolbox.com* adreslerinden yapılabilmektedir.

4.4. Karaliste

Karaliste (Blacklist), bilinçli veya bilinçsiz SPAM e-posta gönderme, virüs saldırısı, hacking vs gibi yasal olmayan eylem yaptığı tespit edilen IP adreslerinin veya e-posta

adreslerinin sunucu üzerinde bir listesinin tutulmasıdır. [28] El il oluşturulan bu listede var olan adreslerden gelen e-postalar, SPAM e-posta olarak reddedilir. Günümüzde halen kullanılan bu yöntem, kaynağı belli olan ve sürekli aynı adreslerden gelen SPAM e-postaların engellenmesinde etkilidir ancak SPAM göndericilerin, geniş bir IP aralığı kullanmaları ve genellikle sahte IP ve e-posta adresi kullanmaları sebebiyle artık yerini gerçek zamanlı karaliste (RBL) servislerine bırakmaya başlamıştır.

Her ne kadar karalistenin tersi bir yöntemle sadece kabul edilecek e-postaların tutulduğu beyazliste kavramı ortaya çıksa da, sadece önceden bilinen adreslerden e-posta alınabileceğinden, tek başına uygulanabilir bir yöntem olarak görünmemektedir. [29]

4.5. Gerçek Zamanlı Karaliste (RBL)

Kullanım şekillerine göre DNSBL olarak da adlandırılan RBL (Realtime Black List), yasal olmayan faaliyetler yapan IP adreslerinin belli süreliğine karalistede tutulması ve daha sonra kendi belirledikleri süre sonunda serbest bırakılmasıdır.

Organizasyon veya kurumlar tarafından tutulan RBL'ler, gelen e-postanın IP adresini ters DNS kontrolüne benzer bir biçimde kendi listelerinde sorgulayarak, listede olması durumunda gelen e-postayı reddetmektedirler. SPAM e-posta gönderdiği rapor edilen e-posta sunucularının listeye eklenmesiyle sürekli güncellenen RBL servislerinin bazı hatalı çıkarımlar üretmeleri mümkündür. Örneğin, tüm dünyadaki IP adreslerini listelerinde tuttukları için genellikle IP adreslerini tek tek tutmayan birçok RBL servisi, 256'lık bloklar halinde bulunan bir IP sınıfı (C sınıfı) içerisinde çok sayıda IP adresi üzerinden SPAM gönderildiği tespit edilirse, o IP sınıfını tümüyle karalistelerine almaktadırlar. Dolayısıyla bu IP sınıfı içerisinde, SPAM olmayan normal e-posta gönderimlerinin yapıldığı IP adresleri de engellenmiş olmaktadır.[28]

Bunların yanında tek bir olumlu yanıta bağlı kalarak e-posta teslimatlarını reddetmek yerine, çeşitli RBL listelerine başvurup her olumlu yanıta bir puan vererek toplam puanın, önceden belirlenmiş bir eşiği aşması durumunda da bu adresten gelen e-postaları reddetmek mümkündür. RBL'lerin bu şekilde kullanımı daha çok Spamassassin gibi filtreleme yazılımlarının kullandıkları yöntemi andırır. [21]

RBL listelerinin bir diğer kullanım şekli de, SMTP aktarımına koşullu gecikmeler konulmuş ise bunların tetiklenmesi için kullanımıdır. Eğer bir IP adresi RBL listesindeyse, bu adresin gönderdiği her komuta bir gecikme ile (örn, 20 saniye) yanıt vermek tercih edilebilir. [21]

E-posta sunucularının herhangibir RBL'de olup olmadığı *http://www.dnsstuff.com/tools/ip4r.ch?ip=* veya *http://www.mxtoolbox.com/blacklists.aspx* adreslerinden kontrol edilebilmektedir ancak bazı RBL organizasyonları bu adreslerden yapılan sorgulara cevap vermemektedir. Bu sebeple gönderilen e-posta karşı tarafa ulaştırılamıyorsa, geri dönen cevapta "blocked, dynamic list" gibi sebebini açıklayan ifadeler ve çözüm için ulaşılabilecek ilgili web sayfası mutlaka verilmelidir. [28]

RBL listelerinin, doğrudan hizmet veren servis sunucularına ulaşarak kullanımı mümkün olabildiği gibi, bu listelerin sürekli güncellenecek şekilde kendi DNS sunucularında kullanılması da mümkündür.[8]

RBL Servisi veren Kurumlar:

- Hotmail, Yahoo vb sunucular
- Maps
- FiveTenSrc
- Uce-Protect
- Apews
- Njabl
- Spamcop
- Nomorefun
- SpamHaus ve Cbl
- Virbl
- Sorbs
- Dsbl
- Dnsbl
- Rbl-TR

4.5.1. Karaliste ve Hotmail , Gmail, Yahoo

Gmail, Hotmail ve Yahoo tamamiyle kendi belirledikleri politikalar gereği işlem yapmaktadırlar. ISP olarak kendi karalistelerini tutarak, MX kaydı ve ters DNS kaydının e-posta sunucuna özel olmasını istemektedirler. Ayrıca bazı alan adları için de SPF kaydının olması istemektedirler.[28]

Bu servislerden gönderilemeyen bir e-postanın sorumlusu, daha önce gönderilmiş olan SPAM e-posta, sözlük saldırısı ya da her türlü saldırı olabilir.[28] Kullanıcının, hizmet veren servise başvurarak vereceği bilgiler doğrultusunda sorun çözülebilmektedir.

4.5.2. Karaliste ve MAPS

SPAM e-posta gönderilmesi, sunucunun açık relay olması veya dinamik IP tanımlaması yapılmasından dolayı karalistesine almaktadır. Duruma göre bir C (256 IP bloğu) sınıfını veya bir B sınıfını (256*256 IP bloğunu) listesine alan bir yapısı vardır.[28]

IP adresinin karalistede olup olmadığı *http://www.mail-abuse.com/cgi-bin/lookup* adresinden sorgulanabilmektedir.

4.5.2.1. Karaliste ve MAPS – RBL

Mail Abuse Prevention Systems (MAPS) tarafından işletilmekte olan bir sistemdir. Serviste açık relay sunucuları olduğu kadar, sadece SPAM e-posta kaynağı olan sunucular da listelenir. E-posta sunucularında seçenek belirtilmeksizin RBL servisinin kullanımı seçildiğinde, varsayılan ayar olarak MAPS-RBL servisinden yararlanıldığından en yaygın kullanılan servistir. [8]

MAPS-RBL özellikle açık relay olmasa bile SPAM e-posta kaynağı sunucuları listelediğinden, listeleme politikası açısından en sıkı olanıdır. Servise başvurmadan önce ilk olarak SPAM e-postaları gönderen kişi veya kurumla temasa geçilmeli, yapılan işin hatalı olduğu anlatılmaya çalışılmalı, son verilmesi istenmelidir. Eğer bundan bir sonuç alınamazsa bir üst sağlayıcıya başvurularak, sistem yöneticileri durum hakkında bilgilendirilmeli ve SPAM e-postaların engellenmesi istenmelidir. Eğer gerekiyorsa ilgili

kişiler SPAM önleme konusunda bilgilendirilmelidir. Bundan da bir sonuç alınamazsa yukarıdaki adımlarda yapılan tüm yazışmalar ve alınan SPAM e-postaları, açık başlık bilgileri ve durumu açıklayan bir rapor ile birlikte rbl@mail-abuse.org adresine gönderilmelidir. Yapılan başvuru MAPS tarafından incelenerek uygun görüldüğü takdirde belirtilen posta sunucusu RBL veri tabanına dahil edilecektir. [8]

Karalistede olunması durumda da karalisteden çıkma talebinin aynı adrese iletilmesi gerekir. Webadresi: *http://www.mail-abuse.org*

4.5.2.2. Karaliste ve MAPS – RSS

Relay SPAM Stopper (RSS) servisi de MAPS tarafından işletilmektedir. RBL servisinden farklı olarak bu serviste, sadece açık relay sunucular listelenir ve veritabanına yapılacak ekleme başvurularında SPAM ve açık relayin kapatılması konusunda daha önce ilgili kuruma başvurulmuş olunması şartı aranmaz. Ancak bir sunucunun açık relay olması, karalisteye girmesi için yeterli değildir, aynı zamanda bu sunucu üzerinden SPAM e-postaların da gönderiliyor olması gereklidir.[8]

Açık relay konumunda olan ve SPAM e-posta gönderen bir sunucunun RSS veri tabanında yer alması isteniyorsa, SPAM e-posta açık başlık bilgisi ile birlikte relays@mail-abuse.org adresine iletilmelidir. Karalistede olunması durumunda da sunucunun relaya kapatılması ve aynı e-posta adresine başvurulması gerekir. Web adresi : *http://www.mail-abuse.org*

4.5.3. Karaliste ve ORBS

ORBS servisi sadece açık relay durumundaki sunucuları listeler. Sunucunun rapor edilmesi için sistem yöneticileri ile konu hakkında görüşülmüş olması gerekmediği gibi, sunucu üzerinden SPAM e-posta gönderiliyor olması da gerekmez.

SPAM e-posta gönderen bir sunucu ORBS veritabanına eklenmek isteniyorsa, başvuru web adresi üzerindeki bir form veya e-posta aracılığıyla yapılabilir. Karalistede olunması durumunda ise, sunucunun relaya kapatılmasının ardından relays@orbs.org adresine başvuru yapılması gerekmektedir. Web adresi : *http://www.orbs.org*

4.5.4. Karaliste ve UCE-PROTECT

Level 1, Level 2, Level 3 seviyesinde, tek IP adresleri ile başlayıp 256*256 IP'lik bloklar halinde karaliste kaydı tutan bir yapısı vardır. IP adresinin karalistede olup olmadığı *http://www.uceprotect.net/en/rblcheck.php* adresinden sorgulanabilmektedir.

IP adresi Level 1 olarak görünüyorsa, bu IP adresinden SPAM e-posta gönderildiği için 1 hafta boyunca bloklanmış demektir.

Eğer IP adresi Level 2 ve Level 3 olarak görünüyorsa, IP adresleri büyük bloklar (30 bin veya Tüm Türkiye) halinde burada listelendiği anlamına gelmektedir. Bu seviyede tüm Türkiye'yi bloklamış bir karalistesi olmasına rağmen e-posta gönderememe problemi ile karşılaşılmamıştır. Bu organizasyona karalisteden çıkmak için başvuru yapıldığında, ücret istenebilmektedir.[28]

4.5.5. Karaliste ve FIVETENSRC

Ters DNS kaydında gerçeklik görmediği zaman tek IP adresini karalisteye almaktadır. SPAM e-posta gönderildiğinin algılanması, ters DNS kaydının uygun biçimde yapılmaması veya A kaydıyla ilgili bir problemden dolayı karalistesine almaktadır.

IP adresinin karalistede olup olmadığı http://www.five-ten-sg.com/blackhole.php adresinden sorgulanabilmektedir.

Ters DNS kaydı düzenlemesinden sonra blackhole18@five-ten-sg.com adresine e-posta gönderilerek çıkarılma talebinde bulunulabilmektedir. [28]

4.5.6. Karaliste ve NJABL

Çoğunlukla ters DNS kaydının olmaması veya yanlış olmasından dolayı tek IP adresini karalistesine almaktadır. Ayrıca sunucunun open relay olmasıda bu karalistede yer almasına sebep olabilir.

IP adresinin karalistede olup olmadığı *http://njabl.org/cgi-bin/lookup.cgi?query=* adresinden sorgulanabilmektedir.

Karalistede olunması durumunda öncelikle dnsstuff adresinden PTR kaydının doğruluğundan emin olunmalıdır. PTR kaydında sorun olması durumunda hizmet alınan ISP'ye başvurarak ters DNS kaydının yapılması istenmelidir. Kayıt düzenlendikten sonra http://njabl.org/remove.html adresinden IP adresi ile bildirim yapılarak, IP adresinin karalisteden çıkarılması için Spamhaus PBL web sitesine başvuru yapılması gerekmektedir. [28]

4.5.7. Karaliste ve SPAMCOP

SPAM e-posta gönderilmesi durumunda tek IP adresini karalistesine almaktadır.
IP adresinin karalistede olup olmadığı *http://www.spamcop.net/bl.shtml* adresinden sorgulanabilmektedir.

Karalistede olunması durumunda, SPAM e-posta gönderimi kesildiğinde, otomatik olarak belli bir süre sonra karalisteden çıkarılacağı belirtilmektedir. SPAM e-posta gönderimi söz konusu olmadığı halde karalistede yer alınması durumunda, 24 saat içinde cevap verilen bir başvuru formu doldurulmalıdır.[28]

4.5.8. Karaliste ve NOMOREFUNN

SPAM e-posta gönderilmesi durumunda tek IP adresini karalistesine almaktadır.
IP adresinin karalistede olup olmadığı *http://moensted.dk/spam/no-more-funn/?addr=* adresinden sorgulanabilmektedir. Karalistede olunması durumunda, sorgulama adresinden başvuru yapılarak birkaç saat içerisinde karalisteden çıkmak mümkündür.

4.5.9. Karaliste ve SPAMHAUS - CBL

SPAMHAUS ve CBL SPAM veritabanını ortak kullanan şirketlerdir. SPAM e-posta gönderildiği tespit edildiğinde tek IP adresini karalistesine almaktadır.
IP adresinin karalistede olup olmadığı *http://cbl.abuseat.org/lookup.cgi* adresinden sorgulanabilmektedir. [28]

Karalistede olunması durumunda, sorgulama adresinden başvuru yapılarak belirtilen süre içerisinde karalisteden çıkmak mümkündür.

4.5.10. Karaliste ve VIRBL

Son 24 saat içerisinde iki farklı SPAM e-posta tespit edilirse karalistesine almaktadır.
IP adresinin karalistede olup olmadığı *http://virbl.bit.nl/search.php* adresinden sorgulanabilmektedir. Karalistede olunması durumunda, sorgulama adresinden başvuru yapılarak karalisteden çıkmak mümkündür. [28]

4.5.11. Karaliste ve SORBS

Bir C sınıfı IP bloğunda, birden fazla IP adresi SPAM e-posta gönderirse 256 sınıfı karalistesine almaktadır.

IP adresinin karalistede olup olmadığı *http://www.de.sorbs.net/lookup.shtml* adresinden sorgulanabilmektedir. Bu listede herkes için tanımlı ters alan adları kabul edilmez olarak tanımlandığından, dinamik karalistesinde olunması durumunda, ters DNS kaydının mutlaka yapılması gerekmektedir. Daha sonra sorgulama adresinden başvuru yapılarak 48 saat içinde karalisteden çıkartılma talebi gerçekleşmektedir.[28]

4.5.12. Karaliste ve DSBL

SPAM e-posta gönderilmesi durumunda tek IP adresini karalistesine almaktadır.
IP adresinin karalistede olup olmadığı *http://dsbl.org/removalquery* adresinden sorgulanabilmektedir.
Karalistede olunması durumunda, sorgulama adresinden başvuru yapılmalıdır. Yapılan başvuruda hizmet alınan ISP'nin onayı istenmektedir. Karalistedeki IP adresinden SPAM e-posta gönderilmediği tespit edilerek gerekli onayın gönderilmesiyle, 24 saat sonra kara listeden çıkmak mümkündür. [28]

4.5.13. Karaliste ve DNSBL

Bu organizasyonda SPAM e-posta nedeniyle karaliste tutar. Ancak bu organizasyonun farkı, birçok dnsbl servisini kullanarak ortak veritabanı oluşturmasıdır.
IP adresinin karalistede olup olmadığı *http://www.dnsbl.net.au/lookup/* adresinden sorgulanabilmektedir.
Birçok farklı dnsbl servisi kullandığından, sorgulanan IP adresinin SORBS, DSBL gibi birden fazla servis tarafından karalistede olması muhtemeldir. Bu durumda listedeki servislere tek tek başvuru yapılarak karalisteden çıkma talebi yapılmalıdır. [28]

4.5.14. Karaliste ve RBL-TR

TASO (Türkiye Anti SPAM Organizasyonu) tarafından Türkiye kaynaklı SPAM e-postaları önlemek için RBL-TR adlı servis yürütülmektedir.

Anti-SPAM organizasyonu kapsamında, halen sürmekte olan anti-SPAM çalışmalarında yararlanılmak üzere RBL servisi işletilmektedir. Servis ana amaç olarak Türkiye kaynaklı SPAM e-postaların önlenmesine yönelik olup, yurtdışından gelen SPAM e-postaların önlenmesi için diğer RBL servisleri tercih edilmelidir.

RBL-TR servisi, benzer diğer servislerde olduğu gibi DNS sorgulaması mantığına göre çalışmaktadır. Bir sunucunun RBL veri tabanında olup olmadığını kontrol etmek için IP.rbl.spam.org.tr adresinin sorgulanması yeterlidir. Sorgulama başarılı olursa sunucu veri tabanında mevcut demektir. Benzer servislerde olduğu gibi, 127.0.0.2 adresi deneme amaçlı olarak sürekli kapalı sunucular listesinde kalacak şekilde ayarlanmıştır. Bu adres deneme amaçlı kullanılabilir; 2.0.0.127.rbl.spam.org.tr adresi 127.0.0.2 adresi olarak çözümlenmektedir. [8]

SPAM kaynağı sunucunun servise eklenebilmesi için aşağıdaki ön şartlar aranmaktadır:

1) Bir sunucunun sadece açık relay olması RBL-TR listesine eklenmesi için yeterli değildir.

2) Sunucunun açık relay olup olmadığına bakılmaksızın üzerinden birden fazla SPAM e-posta gönderilmiş olması gereklidir.

3) SPAM e-postaları alan veya RBL-TR listesine eklenmesi yönünde başvuru yapmak isteyen kullanıcının, SPAM gönderen site yöneticisine başvurmuş olması, başvurunun olumsuz sonuçlanması veya 24 saat içerisinden yanıt alınamamış olması gerekmektedir. Sözü edilen kişi mümkünse bu durumda bir üst sağlayıcı ile görüşerek durumu bildirmeli ve önlem alınmasını istemelidir. [8]

Bu şartlar altında, RBL listesine ekleme istekleri rbl@spam.org.tr adresine en az iki SPAM e-posta örneğini açık başlık bilgisi ile birlikte gönderilmeli, kurum veya kişilerle yapılan görüşmeler bu e-posta ile birlikte gönderilmelidir. Yapılan başvurular incelendikten sonra, belirtilen şartlara uyan sunucular rbl listesine eklenecektir. [8]

Sunucunun listeden çıkarılması için yapılacak başvurularda daha önce meydana gelen e-postaların önlenmesi ve bundan sonra benzer durumların ortaya çıkmasının engellenmesi yönündeki çalışmaların açıklanmış olması gereklidir. Listeye alınmış bir sunucunun listeden çıkarılabilmesi için, daha önce karşılaşılan SPAM e-postalar bu yolla gönderilmiş olmasalar dahi, sunucunun relay'e kapalı olması şartı aranacaktır. Listeden çıkarılma başvuruları yine rbl@spam.org.tr adresine iletilmelidir. [8]

4.6. Gönderici Yetkilendirme Şemaları

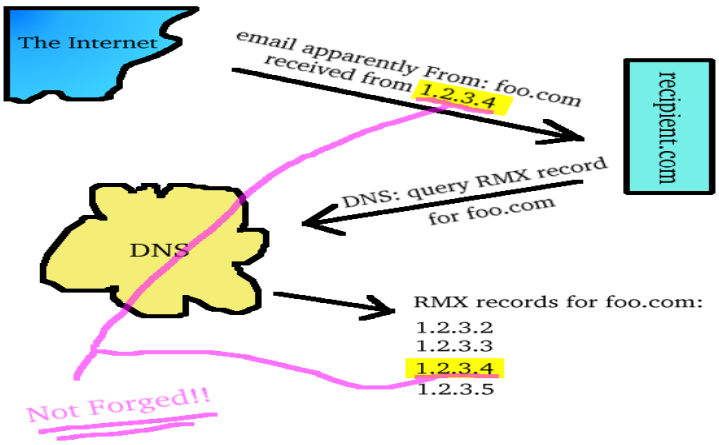
Daha önce bölüm 2'de bahsedildiği gibi SMTP protokolünün kullanılmaya başlandığı ilk dönemde bir e-posta, herhangi bir e-posta sunucusu üzerinden gönderilebilmekteydi. Bu durumun güvenlik açıklarına sebep olmasından dolayı, gönderici ve alıcı tarafındaki hedef sunucular arasında oluşturulan kanal sayesinde daha güvenli aktarım sağlanmıştır. Ancak günümüzde tüm sunucuların relay ve ters DNS kayıtları düzgün olmadığından eski durum da halen devam etmektedir. Bu sebeple güvenlik açığı olan bu sunucular SPAM göndericilerin hedefi haline geldiğinden, gönderici kimliğinin doğrulanmasını sağlayacak çeşitli yöntemler geliştirilmiştir. Bu yöntemler genel olarak alan adı sahibinin, e-posta göndericilerini yetkilendiren kuralları içermektedir.

İlk olarak Paul Vixie tarafından MAIL-FROM MX kayıtları tasarlanmış ve daha sonra yapılan çalışmalarla farklı şemalar geliştirilmiştir.[21] Bunlar:

- RMX (Reverse Mail Exchanger)
- RMX++
- Gönderici Yetkilendirme Dizgesi (Sender Policy Framework)
- E-postalar için Microsoft Çağrı Kimliği

4.6.1. RMX

Hadmut Danisch tarafından tasarlanmış ve yayınlanmış bir şemadır. DNS'e ek olarak RMX kayıtları bulunmaktadır. Bu şema altında, kullanıcı@alanadı.dom adresli tüm e-postalar alanadı.dom'un DNS kayıtlarında bulunan yerlerden gelmek zorundadır.[21]



Şekil 25 – RMX Kayıt Sorgulaması [25]

4.6.2. RMX++

RMX'in tasarımcısı olan Hadmut Danisch tarafından geliştirilmiştir. RMX++, HTTP sunucular üzerinden özdevimli yetkilendirmeyi mümkün kılar. Alanadı sahibi DNS üzerinden bir sunucu belirtir ve e-posta alıcısı bu sunucuya bağlanarak göndericinin geçerliliğini saptamak için oradan bir yetkilendirme kaydı elde etmeye çalışır. Bu şema alanadı sahibine gönderici adreslerini yetkilendirmede kullanılacak kuralları daha ayrıntılı belirleme imkanı verir.

Hadmut'un verdiği bir örnekte, hergün iş saatleri dışında belli bir adresten beş e-postadan fazlasına izin vermeyen bir yetkilendirme sunucusunun bu sınır aşıldığında bir uyarı vereceğini bildirmesine karşın; Rick Stewart'a göre, RMX++'nın özdevimli doğası bir başarısızlığın nedenlerinin bulunmasını zorlaştıracaktır. Eğer günlük beş e-postalık bir sınır varsa, bu sınır, tek bir e-postanın beş kere sınanması ile dolacaktır. Yani şema, bir e-postanın defalarca sınanmasına imkan vermemektedir. [21]

4.6.3. Gönderici Yetkilendirme Dizgesi (SPF)

SPF (Sender Policy Framework), gönderici yetkilendirme için en iyi bilinen şemalardan biridir. SPF bilgisi bir alan adının üst düzey DNS kayıtları arasında bir "txt" kaydı olarak görünür. Bu kayıt, alan adı kullanıcısının e-posta gönderimini sadece bu kaynaktan yaptığını ve eğer başka bir kaynaktan bu kullanıcı adıyla e-posta gönderilirse e-postanın sahte olduğunu ifade eder.[21] Geliştirilmesi süren bu txt kaydı, bir v=spf1 dizgesi ile başlar ve aşağıdaki belirteçlerden bazıları ya da hepsi ile kullanılabilir: [21]

- a - geçerli gönderici makine bu alan adının kendi IP adresidir.
- mx - bu alan adının e-posta alıcıları, ayrıca geçerli göndericilerdir.
- ptr - eğer gönderenin IP adresi için ters DNS kaydındaki isim, gönderici adresin alan adı kısmındaki isimle eşleşiyorsa, gönderen yer geçerli göndericidir.
- Bu belirteçlerin her birinin önüne bir yetkili kaynak olduğunu belirtmek için varsayılan olan bir artı işareti, yetkisiz olduğunu belirtmek için bir eksi işareti, yetki bakımından nötr olduğunu belirtmek için soru işareti veya yetkisiz olarak değerlendirilebilineceğini belirtmek üzere bir yaklaşık işareti (~) konabilir.

Her belirteç ':' (iki nokta üst üste) işaretinden sonra bir alan adı belirtmek üzere kullanılabilir. Örneğin, bir Comcast müşterisiyseniz, sizin DNS kayıtlarınız arasında "v=spf1 -ptr:client.comcast.net ptr:comcast.net -all" şeklinde bir txt kaydı olabilir. Bu kayıt, bu alandan posta gönderen makinenin IP adresi çözümlendiğinde elde edilen isim birşey.client.comcast.net şeklindeyse bu adres yetkisizdir, birşey.comcast.net şeklindeyse yetkilidir, belirtilenler dışında kalanlar da yetkisizdir ("-all") anlamına gelir.

Her alan adı için bir SPF kaydı bulunmalıdır. Bazı büyük siteler artık bu kaydın bulunmadığı alanlardan posta kabul etmemektedir. Gönderici yetkilendirme şemaları genelde kabul görmemiş olmasına rağmen SPF evrensel olarak büyük oranda kabul görmüştür. SPF'ye karşı çıkanlar, alan adı sahiplerinin posta gönderen müşterileri/kullanıcıları üzerinde bir tekel kurmak için bunu kullanabileceklerini ileri sürmektedirler.[21][30]

4.6.4. E-Postalar için Microsoft Çağrı Kimliği

Kurallarının gönderici alan adının DNS bilgileri arasında bir TXT kaydı olarak görünmesi bakımından SPF'ye benzer. Ancak, basit anahtar kelimeler yerine, XML olarak kodlanmış oldukça geniş kapsamlı bilgilerden oluşur. Bu XML şeması Microsoft tarafından bir lisans altında yayınlanmıştır.

SPF, bir e-postanın sadece gönderici adresine bakarak çalışırken, XML şeması e-postanın mesaj başlıklarını değerlendiren bir araç olarak çalışır. Böyle bir sınamanın SMTP aktarımında yapılabileceği en erken nokta, e-posta verisi alındıktan sonra ve son 250 yanıtını göndermeden öncedir.[21]

4.7. SPAM E-Posta Engelleme Yazılımları

4.7.1. Bayes filtreleri

Temeli İngiliz istatistikçi Thomas Bayesian tarafından geliştirilen Bayes Teoremi'ne dayanan bu yöntem, Paul Graham'ın 2002 yılında yazdığı makalede SPAM e-posta filtrelemede bu teoremin kullanılabilirliğine değinmesiyle SPAM e-postalarla mücadele konusuna yeni bir boyut kazandırmıştır. Graham'a göre alınan her e-postaya, mesaj başlığındakiler de dahil olmak üzere içerdiği kelimeler incelenerek 0 ile 1 arasında bir SPAM skoru atamak mümkündür. Bu sayının hesaplanabilmesi için öncelikle gelen çok sayıda SPAM ve SPAM olmayan e-postaların ayrı ayrı incelenmesi ve filtrenin eğitimi için kullanılması gerekmektedir. Bu inceleme sonucunda eğer belli bir karakter veya kelime sadece SPAM olan e-postalarda rastlanıyorsa o karakter veya kelimenin geçeceği bir sonraki e-postanın da SPAM olma olasılığı çok yüksek olacaktır. Aynı şekilde, büyük

bir çoğunlukla gerçekten okunmak istenen e-postalarda rastlanan karakter veya kelimelerin daha sonra SPAM içermeyen e-postalarda görünmesi beklenir.[8] Bayes filtrelerinin eğitimi için ne kadar çok SPAM ve SPAM olmayan e-posta kullanılırsa başarı oranı da o derece artmaktadır. Yayınlanan birçok raporda iyi eğitilmiş bir bayes filtresinin %99 gibi önemli bir başarı sağladığı bildirilmektedir. [29]

Bayes filtrelerinin kelime indeksleri çoğunlukla eğitildikleri dile hatta kullanıcıya özeldirler. Bu bakımdan sistem çapında ve SMTP aktarımı sırasında yapılan filtrelemeden ziyade kişisel içerik filtrelemesine uygundurlar. Bununla birlikte e-postalar sunucuya hatta kullanıcıya kadar ulaşabildiğinden SPAM e-postaların oluşturduğu trafiği önleme açısından bir etkinliği yoktur. Bir e-postanın SPAM olup olmadığı kişiden kişiye değiştiğine göre bayes filtrelerinin kullanıcıya özgü olması en önemli avantajlarından biri olarak kabul edilebilir. Ancak SPAM göndericiler e-postalarına kısa hikayeler ve sözlükten rastgele seçilmiş kelimeler ekleyerek basit bayes filtrelerini de etkisiz kılacak teknikler geliştirmişlerdir. Bu durum, bayes filtrelerinin atadığı SPAM puanını düşürerek uzun vadede bayes indeksinin kalitesini düşürmektedir.[21]

Bogofilter, SpamBayes, ASSP ve DSPAM bayes filtre yöntemiyle çalışan yazılımlara örnektir. Spamassassin 2.5 ve Mozilla Thunderbird posta istemcisi de 1.3 sürümünden itibaren, Bayes filtre yöntemiyle SPAM kontrol özelliği sağlamıştır.

4.7.1.1. Bogofilter Bayes Filtresi

Bogofilter, Eric Raymond tarafından C programla dilinde yazılan ve Bayes Olasılık Teoremi'ni esas alan açık kaynak kodlu bir yazılımdır.[8] Kullanıcılara gelen e-posta trafiği içinden SPAM e-postaları ayırmak için e-postalar bogofilter tarafından filtrelenmekte ve SPAM olduğu belirlenenler işaretlenmektedir.[31]

Bogofilter, filtreleme işlemi sırasında BerkeleyDB veritabanı kullanmaktadır.[8] Bu veritabanı, daha önce bogofilter'a tanıtılmış olan SPAM ve SPAM olmayan e-postalardan oluşmaktadır. Gelen e-postalar parçalara ayrılıp bu veri tabanı ile karşılaştırılmakta ve SPAM olma ihtimali belli bir eşik değerinin üzerinde çıkanlar SPAM olarak işaretlenmektedir. Veri tabanı içerik olarak ne kadar zengin ve güncel olursa başarı oranı o derece artmaktadır. Ancak bogofilter kullanıcıya özgü bir filtreleme yöntemi

olduğundan, kullanıcı sayısının çok fazla, kullanıcıların aldığı e-postaların da çok çeşitli olduğu bir ortamda gelen SPAM e-postaların filtrelenme başarısı düşmektedir. [31]

Bogofilter ile SPAM olarak işaretlenen e-postaları silmek veya kullanıcının farklı bir klasörüne taşımak mümkündür. [8] Bogofilterın ilk eğitim aşamasında SPAM olarak işaretlenen e-postaları bir klasöre taşımak olabilecek hataları kontrol edebilmek açısından önemlidir.

4.7.2. Spamassassin

Spamassassin kural tabanlı bir SPAM e-posta engelleme aracıdır. Spamassassin 800'den fazla kuralı içinde barındırmakta ve bu kurallara göre bir e-postanın SPAM olup olmadığına karar vermektedir. Esnek ve gelişmiş programlama arabirimi sayesinde hemen hemen tüm e-posta sunucuları ile çalışabilmektedir. Ayrıca Razor, Pyzor ve Dcc gibi birçok SPAM e-posta önleme araçlarıyla birlikte bir bütünlük içinde çalışabildiği gibi RBL'leri (kara listeleri) kontrol edebilmekte ve MX kaydı sorgulaması yapabilmektedir.[32]

Çalışma mantığı kısaca, e-postanın başlık bilgisi, konu ve gövde kısmının SPAM kontrolünden geçirilmesi şeklindedir. Kontrol sırasında her bir olası SPAM işareti için puanlar verilmektedir. Örneğin e-postanın konu kısmı boşsa veya büyük harfler içeriyorsa, e-posta gövdesi çok fazla HTML etiketi içeriyorsa ya da e-posta birden çok kişiye gönderilmişse gibi kriterler göz önünde bulundurulmaktadır. Bir de bunlara RBL ve MX kontrolü eklenebilmektedir. Bunların sonucunda yapılan puanlama, belirlenen eşik değere göre SPAM ya da SPAM değil şeklinde sonuçlanmaktadır.[32] Spamassassin 2.5 ve sonraki sürümlere Bayes tabanlı öğrenme özelliği de eklenerek bilinen SPAM e-postaların taranarak kullanıcı tarafından alınan SPAM e-posta karakteristiğinin tanımlanmasına imkan sağlanmıştır. Ayrıca beyazliste ve karaliste tanımlamaları yapılabildiği gibi, olası SPAM işaretlerinin değerlendirme puanlarında kişisel ağırlıklandırma yapılabilmektedir.[33]

Puanlamada kullanılabilecek olası SPAM işaretleri aşağıdaki gibi ifade edilebilir.

- Değiştirilmiş, hileli veya tipik SPAM özellikleri taşıyan e-posta mesaj başlığı.
- Başlıkta SPAM programlarına ilişkin anahtar kelimeler.
- İçerikte tipik kelime veya kalıplar.
- İçerikte sıra dışı formatlama.
- Karalistelere kayıtlı göndericiler.
- Dağıtık SPAM listeleyicilerine kayıtlı sistemler. (Razor, Pyzor, DCC)

Olası SPAM işaretleri değerlendirilerek bir e-posta için aşağıda verilen örnekteki gibi ağırlıklı bir "SPAM Notu" tespit etmek mümkündür.

- Kime: alanı boş bırakılmış (1 puan)
- E-postanın içinde FREE kelimesi geçiyor (1 puan)
- Konu: alanında sadece büyük harf kullanılmış (1 puan)
- E-posta içinde üçten fazla renk kullanılmış (0.5 puan)
- Sistem karalistelerde kayıtlı (2 puan)

Belirlediğimiz eşik değerin 5 puan olduğunu varsayarsak bu e-posta toplam 5.5 puana ulaştığından dolayı SPAM olarak kabul edilecektir. SPAM olarak belirlenen bir e-postayı silmek, önlem olarak kullanıcının farklı bir klasörüne aktarmak ya da çeşitli şekillerde işaretlenerek kullanıcının kararına bırakmak mümkündür. [33]

Spamassassin, %1 civarında hata çıkarımına sebep olsa dahi, e-postaların SPAM olup olmadıklarını %98'in üzerinde doğru bir şekilde tespit etmesi ve son kullanıcılara özgü ayarlanabilir olmasıyla ön plana çıkmaktadır. Bunun yanında kuralların oldukça fazla olması sebebiyle sistem kaynaklarını yoğun bir şekilde kullanması ve yavaşlığı Spamassassin'ın olumsuz yönleri olarak ifade edilebilir.[33]

4.7.3. SPAM E-Posta İmza Depoları

SPAM e-postayı diğerlerinden ayıran bir özellik, çok sayıda adrese gönderilmiş olmasıdır. Bir e-posta daha önce belli bir sayıdaki kullanıcı tarafından SPAM olarak işaretlemişse, e-

postanın sonraki teslim aşamasında, e-postayı kabul edip etmemek noktasında bu fiili durumun kullanılmasına imkan sağlayan yazılımlardır. [21] Bu yazılımlar:

- Razor
- Pyzor
- Distributed Checksum Clearinghouse (DCC)

Bu yazılımlar sadece SPAM e-posta olduğu bilinen bir e-postanın bir eşdeğer kopyası alındığında tetiklenen basit imza sınamaları yaparak çalışırlar. Bunlar e-posta içinde bilinen kalıpları arayarak değil, e-posta mesaj başlığındaki ve gövdesindeki belli değişiklikleri hesaba katarak değerlendirme yaparlar.[21]

4.7.3.1. Razor

Kullanıcılara daha önce gelmiş olan SPAM e-postaları merkezi Razor sunucusuna bildirmesi ve daha sonra gelen e-postaların önceki e-postalarla karşılaştırılması esasına göre çalışır. SPAM e-postaların gövde karakteristikleri, daha sonra gelen e-postalarla karşılaştırılmak üzere Razor sunucusunda depolanır. Üzerinde Razor kurulu olan e-posta sunucusu bir e-posta aldığında bu e-posta, Razor sunucusundan sorgulanır. Eğer e-posta Razor sunucusunda daha önce SPAM olarak kaydedilmişse, e-posta SPAM olarak işaretlenir. Bu SPAM e-postalar değiştirilmeksizin farklı binlerce kişiye gönderildiğinden, ilk alıcının bu e-postayı Razor veritabanına eklenmesini sağlamasıyla sonraki alıcıların bu e-postayı engellemesi sağlanır. Spamassassin'le birlikte kullanıldığında başarısı %95'e kadar çıkmaktadır.[32]

4.7.3.2. Pyzor

Pyzor gelen e-postaların belirli sunucular üzerinden kontrol edilip SPAM e-posta olup olmadığını sorgular. [34] Python dilinde yazılmıştır ve GPL lisansına sahiptir. Razor gibi çalışır ancak veritabanının Razor kadar güçlü olduğu söylenemez. Spamassassin ile birlikte çalışabilmektedir.[32]

4.7.3.3. DCC (Distributed Checksum Clearinghouse)

DCC sunucu-istemci mantığıyla çalışan bir yapıdadır. Çalışma şekli olarak Razor ve Pyzor'la aynı prensiplere dayanmaktadır. Alınan her e-posta DCC sunucularındaki SPAM veritabanı ile karşılaştırılır. Sorgulama sonucuna göre e-postanın SPAM olup olmadığına karar verilir. Razor ve Pyzor'la beraber aynı sunucuda çalışabilir. Fakat tüm bu araçların aynı anda çalışması sunucu performansını ve İnternet bant genişliğini önemli ölçüde düşürecektir. Gelen her bir e-posta için İnternetten bu uygulamaların sunucularına bağlanılacak ve sorgulama yapılacaktır. DCC, Spamassassin'le birlikte çalışabileceği gibi sendmail ile doğrudan bütünleştirilebilmekte ya da ProcMail gibi bir e-posta süzücü ile de çalıştırılabilmektedir.[32]

4.7.4. Resim İçerikli SPAM E-posta Filtreleri

Resim içerikli SPAM e-postaların filtrelenmesine yönelik birçok çalışma yapılmıştır. Bu çalışmalardan biri resim içeriğinin optik karakter tanıma (OCR) yazılımları yardımıyla metne çevrilmesidir. Resim içeriğinden çıkartılan metin daha sonra klasik metin tabanlı bir SPAM filtresine iletilir ve bu filtre tarafından içeriği istatistiksel olarak incelenir. Bu yöntemin başarısı ne yazık ki kullanılan optik karakter tanıma sisteminin başarı katsayısı ile doğru orantılıdır ve bu sistemin başarısız olduğu noktalarda kullanımı güçleşmektedir. Dahası optik karakter tanıma sistemlerinin özellikle günümüzde insanların birbirleriyle giderek daha sık paylaşmaya başladıkları fotoğraflar gibi yüksek çözünürlükte resimler üzerinde çalışırken aşırı yüklenmeleri bu sistemlerin kullanımını pratikte oldukça zorlaştırmaktadır.[22]

Bir başka çalışma ise histogram analizi ile filtreleme yöntemidir. Bu çalışmada, SPAM göndericisinden gelen e-posta, sunucu tarafından filtreye gönderilir. Bu aşamada devreye giren python kodu, gelen e-posta içinden resmi alır. Ardından gri ölçekli pgm formatına dönüştürülen resmin histogramı çıkarılır. Gönderilen resim içerikli SPAM e-postaların en karakteristik özelliği beyaz arka plana sahip olmaları ve çok az renk kullanılmış olmasıdır. Oluşturulan histogram datasında kullanılmayan renkleri ifade eden 0 sayısı ile diğer sayılara göre çok daha fazla karşılaşılması, bir SPAM olma işareti olarak kabul edilmiştir. Buna ek olarak, çizilen histogramlarda tepe noktası olarak kabul edilen, en çok

karşılaşılan renk bilgilerinin, diğer renklere olan baskınlığının da SPAM olma belirtisi olduğu ortaya çıkmıştır. Bu yöntemle, sunucuya gelen resim tabanlı spam e-postalarının filtre tarafından yakalanma oranı %81 olarak tespit edilmiştir.[22] Her ne kadar bu gibi birçok farklı filtreleme yazılımı geliştirilse de, Spamassassin, RBL ve Razor gibi yöntemler halen resim içerikli SPAM e-postaları engellemenin etkin yollarındandır.

4.7.5. URL İçerikli SPAM E-Posta Filtreleri

Tipik bir URL bağlantısına bakılarak ilgili e-postanın istenen bir e-posta olup olmadığına karar verilebilir. Greenview Data, Inc. şirketi SPAM e-postaları filtrelemek amacıyla kesin bir tespit yöntemi uygulamıştır. Bu yönteme göre 24 saat boyunca sürekli SPAM e-postaları gözleyen son derece eğitimli personel ile URL'lerin önemli olup olmadıklarını ve eklenen URL'lerin doğruluğunu tespit etmektedirler. Bununla birlikte, farklı URL'lerin çok hızlı bir şekilde artması yüzünden bakım ve onarım maliyeti çok hızlı bir biçimde artmış ve bu maliyet artışı son kullanıcılara bir maliyet olarak yansımıştır.[35]

Bilinen açık kaynak kodlu bir anti-SPAM yazılımı olan Spamato, üç farklı URL içerikli SPAM filtreleme olanağı sağlamaktadır. Bunlar, Razor Filtresi, Domainator ve Early Grey Filtresidir. [35]

Razor Filtresi Whiplash algoritmasını kullanarak URL'lerin daha önceden kara listeye alınıp alınmadıklarının kontrolünü gerçekleştirmektedir. Her alan adındaki SPAM bulunma olasılığı Razor ağ analizi ile değerlendirmeye tabi tutulmaktadır. Bu yaklaşımın dezavantajı Razor ağına bildirilen SPAM e-postaların çoklu URL içeren e-postalarla birlikte bildirilmesi sonucunda bazen karışıklık oluşturmasıdır. Ayrıca, Razor ağına bağımlılığı yüzünden bu tekniğin kullanımı online işlemlerin yapılma kabiliyetini azaltmaktadır. Bunun yanında geçmiş dönemde karalisteye alınan URL'lerdeki SPAM olmayan normal URL çoğunluğu sebebiyle yanlış uygulamalara da sebebiyet verebilmektedir. [35]

Dominator, alan adına referans olabilecek web sayfalarının sayısını tespit etmek amacıyla google arama motorunun veri tabanına ihtiyaç duymaktadır. Bu uygulama mevcut veritabanının bakım maliyetini önemli bir ölçüde düşürmekle birlikte araştırma ve genel

değerlendirme maliyeti göz ardı edilemeyecek ölçüde yüksektir. Online uygulama işlemlerinde uygulanamamaktadır.[35]

Bir başka URL içerikli filtreleme yöntemi olan Earl Grey filtresi gelen e-postalardaki URL ve alan adlarını, SPAM olarak listelenen sunucular üzerinde kontrol eder. Hash algoritmasının kullanılması sebebiyle, devamlı olarak girilen sahte alan adları parmak izlerini değiştirmektedirler. Bu durum e-postanın tanınabilirliğini imkansız hale getirebilmektedir. [35]

4.7.6. SpamGuard

SpamGuard, MTA log dosyalarını kullanıcının belirleyeceği bir periyotta, örneğin 10 dakikada bir "from" kısmına göre tarar. Eğer from'daki e-posta adresi belirlenen zaman içerisinde yine kullanıcının belirlediği bir eşik değerinden daha fazla log dosyasında geçiyorsa SpamGuard bu adresi karaliste dosyasına ekler. Böylece bu kullanıcıdan gelecek sonraki bütün e-postalar engellenerek SPAM e-postaların yayılması önlenmiş olur.

SpamGuard'ın istenilen kullanıcılar için bir eşik değeri vazifesini görecek ve bu kullanıcıya istediği kadar e-posta atmasını sağlayacak bir yapısı da mevcuttur. Bu şekilde istenen kullanıcıların fazla e-posta trafiği yapmasını SpamGuard görmezlikten gelecektir.[36]

4.7.7. qSheff

QSheff, qmail e-posta kuyruğuna girecek e-postaların virüs ve SPAM e-posta filtreleme programları tarafından kontrol edilebilmesi için bir ara programdır. Problemsiz olarak içerik taramasından geçen e-postalar qmail kuyruğuna verilerek yoluna devam etmesi sağlanır. Basit ve güçlü algoritması ile yüksek performans sağlamaktadır.[34] Ayrıca e-postaları kuyruğa girmeden kestiğinden dolayı e-posta sunucusunun yükünü büyük oranda azaltmaktadır. qSheff'in sunduğu özellikler şunlardır: [36]

- Karantina (Virüslü veya SPAM'lı e-postaları saklayabilme)
- Değişik antivirüs ve anti-SPAM yazılımları ile birlikte çalışabilme

- Konuya göre filtreleme, düzenli ifade desteği
- Karaliste, virüs veya SPAM bulunduğunda geriye dönmeme, karaliste seçeneği
- Kolay kurulum ve kolay yönetim
- Beyaz/Karaliste oluşturabilme (ağ, IP, alan adı ve e-posta adres bazlı yasaklama veya geçirme)
- Bozuk başlıklı e-postaları kesebilme
- Detaylı günlük tutma
- MRTG ile SPAM trafiğini görüntüleyebilme
- Kolay hata ayıklama, hata takibi
- Gelişmeye açık, hızlı ve basit kod [36]

QSheff, e-postaların parçalanması için ripmime yazılımına ihtiyaç duymaktadır. Ripmime, e-postaları başlık, gövde ve ekler şeklinde ayrı ayrı dosyalara böler. Bu sayede SPAM e-posta kontrolü yapılırken başlık, gövde ve eklerdeki bilgiler ayrıştırılarak kontrol edilebilmektedir.[34]

4.7.8. Zabit

Zabit, qSheff veya qscanq gibi alternatif kuyruk tetikleyicileri ile çalışabilen içerik filtreleme ve eklenti kontrol yazılımıdır. Yazılımın çalışabilmesi için öncelikle kuyruk tetikleyici bir yazılımın e-posta sunucusunda kurulu olması gereklidir. Gelen e-postalar ripmime ile başlık, gövde ve eklerine ayrılarak zabit kontrolünden geçerek SPAM olması durumunda e-posta reddedilir.[36]

4.7.9. SpamPal

Spamhaus, ORBD, SpamCop, DSBL, SORBS, Spambag gibi güvenilir SPAM karaliste veritabanlarını kullanan SpamPal, gönüllü bir kullanıcı kitlesi tarafından hazırlanmıştır. Uygulama kullanıcıya yönelik olup Outlook Express, Outlook, Eudora vs. POP3 e-posta programları ile birlikte çalışmaktadır. SpamPal arka planda çalışarak POP3 trafiğini dinler ve tespit ettiği SPAM e-postaların konu kısımlarının başına ***SPAM*** ifadesini ekleyerek işaretler. Böylece e-posta programında bir filtre oluşturarak işaretlenmiş e-postaların gelen kutusuna gelmeden silinmesini sağlamak mümkün olmaktadır. Ayrıca

Spampal tarafından silmesi istenmeyen e-postalar için beyazliste hazırlamak mümkün olduğu gibi e-posta gelmesi istenmeyen yerler için de karaliste tutma imkanı sağlanmaktadır.

4.8. Antivirüs

Antivirüs, zombi ve dolayısiyla Botnet oluşumunu engellemenin bir yöntemi olarak görülebilir. Botnetlerin dünya genelinde sebep olduğu SPAM e-posta trafiği düşünüldüğünde Botnet oluşumu ne derece engellenebilirse SPAM e-postaların da o derece azalması kaçınılmazdır. Bu sebeple virüs taraması, genel bir SPAM e-posta engelleme çözümü oluşturmada etkili bir araçtır. Dolayısıyla bir organizasyonun tüm kullanıcı ve sunucularının güncel bir antivirüs uygulamasıyla güvenli bir sisteme dönüştürülmesi çok önemlidir.

4.8.1. Clamav Antivirus

Clamav unix dünyası için tasarlanmış açık kaynak kodlu bir antivirüs yazılımıdır. Kolay kullanımı ve esnek yapısı sebebiyle çok tercih edilmektedir. Özdevimli virüs veritabanı güncelleme özelliğine sahiptir. Otuz binden fazla virüs tanıyabilmekte ve birçok e-posta sunucusu ile bütünleşik olarak çalışabilmektedir. Özellikleri kısaca şu şekildedir:[32]

- GNU GPL lisansına sahiptir.
- POSIX Uyumludur.
- Erişim Tarama (Access Scaning) özelliğine sahiptir. (Yanlızca Linux ve Free BSD)
- Arşiv dosyalarını ve sıkışmış dosyaları tarayabilir.(Zip, rar, tar, gzip, bzip2, Ms OLE2, MS Cabinet Files, MS CHM, MS SZDD)
- Güçlü bir e-posta tarayıcıya sahiptir.
- Güncellemesi kolaydır. [32]

4.9. SMTP Aktarımının Geciktirilmesi

SPAM gönderimini durdurmanın etkin yollarından birisi de SMTP aktarımı sırasında aktarıma gecikmeler koymaktır. Virüs içerikli e-postaların hemen hepsi ve SPAM e-postaların çoğu, kısa sürede çok yüksek miktarlardaki e-postayı göndermek üzere amaca uygun hale getirilmiş SMTP istemci yazılımları sayesinde alıcının e-posta sunucusuna doğrudan doğruya teslim edilirler. Bu yazılımların asıl hedefleri, özellikle yavaş yanıt veren e-posta sunucularıdır. E-posta sunucusu daha SMTP aktarımına hazır olduğunu belirtmeden, sunucuya bir HELO veya EHLO komutu gönderilir ve/veya sunucunun PIPELINING yetisini ilan etmesini beklemeksizin ard arda çeşitli SMTP komutlarıyla bağlantı kurmayı denerler.[21]

Alıcı tarafındaki e-posta sunucusu SMTP aktarımının hemen başında aktarıma hazır olduğunu belirtmeden önce, DNS karaliste sorgulamaları gibi zaman kaybına sebep olan bazı sorgulamalar yapıyorsa, bu yazılımlar e-posta sunucusunun biraz zamana ihtiyacı olabileceğini dikkate almadıklarından amaçlarına ulaşamadan bağlantı kesilir.

Ek gecikmeler koyarak da bu durumun oluşmasına yardımcı olmak mümkündür.

• SMTP aktarımına hazır olduğunu bildirmeden önce 20 saniye,
• Selamlaşmadan (EHLO veya HELO) sonra 20 saniye,
• MAIL FROM: komutundan sonra 20 saniye ve
• Her RCPT TO: komutundan sonra 20 saniye.

RFC 2821 göndericinin her SMTP yanıtı için birkaç dakika beklemesini zorunlu kılar. Bazı alıcılar, gelen e-posta teslimat bağlantılarına yanıt olarak Gönderici Varlık Sınaması uygularlar. Böyle bir alıcıya e-posta gönderildiğinde, bu alıcı göndericinin alan adı için yetkilendirdiği posta alıcısına bağlanıp gönderici adresinin doğrulanmasını sağlamak üzere bir SMTP diyalogu başlatacaktır. Böyle bir Gönderici Varlık Sınaması için varsayılan zamanaşımı süresi 30 saniyedir. Eğer konulan gecikme süresi bu sürenin aşılmasına sebep oluyorsa, istemcideki Gönderici Varlık Sınaması başarısız olacağından gönderilen e-posta teslimatı reddedilebilecektir. Bu sebeple normal e-posta aktarımı ile ilgili girişimin başlamasını geciktirilebilecek en uzun süre 20 saniyedir. [21]

4.10. Sözlük Saldırılarının Önlenmesi

Sözlük Saldırısı (Dictionary Attack), çok kullanılan isimleri bazen alfabetik, bazen ters alfabetik bazen de rastgele seçilmiş isimler şeklinde RCPT TO: komutlarıyla deneyerek alıcı adreslerinin saptanması şeklinde gelişen SMTP aktarımlarıdır. [21]

Sözlük saldırılarıyla mücadele etmenin en etkin yolu, her başarısız adreste aktarım gecikmesini arttırmaktır. Örneğin, mevcut olmayan ilk alıcı adresi için bekleme süresi 20 saniye, ikincisinde 30 saniye, 3. için 40 saniye, ... gibi.[21]

4.11. Dolaylı SPAM E-Postaların Engellenmesi

Çoğu zaman dolaylı SPAM e-posta, antivirüs tarayıcılarının ürettiği virüs uyarıları şeklinde karşımıza çıkar. Bu virüs uyarılarının 'Konu' satırı dahil birçok karakteristik özelliği antivirüs yazılımının kendisi tarafından oluşturulur. Dolayısıyla, ortak karakteristik özelliklerin bir listesini yaparak bu tip hatalı virüs uyarılarını filtrelemek mümkündür. Spamassassin ile kullanmak üzere böyle bir hatalı virüs uyarı listesi hazırlanmıştır. Tim Jackson tarafından hazırlanan bu listeye *http://www.timj.co.uk/linux/bogus-virus-warnings.cf* adresinden ulaşılabilmektedir.[21]

Dolaylı SPAM e-postalara yol açan diğer bir durum olan Teslimat Durum Bildirimlerini engellemek için ise SPF kaydı kullanılmalıdır. Gönderici Yetkilendirme Dizgesi (SPF)'nin amacı özellikle geçerli bir e-posta adresinin taklit edilmesini önlemektir. Eğer alan adı ile DNS bilgileri arasında bir SPF kaydı varsa, SPF sınamaları yapan alıcılar, taklit edilmiş adreslerle gönderilmiş e-postaları kabul etmeyecektir. Böyle bir durumda da, bu alan adı adreslerine bir Teslimat Durum Bildirimi gönderilmeyecektir.[21]

4.12. Honeypots

Honeypots, bilgi sistemlerini yetkisiz kullanmaya çalışanları saptamak ya da caydırmak amacıyla kurulan bir tuzaktır. Genelde saldırgan açısından değerli olabilecek bir bilgi içeriyormuş gibi görünen bir bilgisayardan, bir veri parçasından ya da bir ağ parçasından

oluşur ve bir ağın parçasıymış gibi görünmesine rağmen ağdan yalıtılmış ve korunmuştur.[21]

Benzer şekilde SPAM göndericileri tuzağa düşürebilmek amacıyla da kullanılan bu yöntemde gerçek bir son kullanıcıya ait olmayan sahte e-posta adresleri oluşturulur. Bu sayede normal e-postaların gönderilmeyeceği bu sahte e-posta adres veya adreslerine gönderilen e-postaların SPAM olduğu kesinlik kazanacaktır. SPAM göndericilerin tespit edilen adresleri toplanarak SPAM veri tabanı oluşturmada kullanılmaktadır. Ayrıca Project Honey Pot sistemi bu adresleri kullanarak web sitelerinden e-posta adresi toplayan robot yazılımların izini sürerek bunları kayıt altına almaktadır. Web tabanlı e-posta hizmeti veren servis sağlayıcılardan biri olan Hotmail 13,000 adet tuzak e-posta hesabı kullanmaktadır. [37] SPAM göndericileri ve SPAM trafiğini analiz etmek için kurumsal bir e-posta sunucusunda yapılan bir çalışmada ise, SPAM göndericilere karşı kurulan bir tuzak yardımıyla Ocak 2006 ile Şubat 2007 tarihleri arasında 400 bin SPAM e-posta tespit edilmiş ve yakalanmıştır.[38]

4.13. Ücretlendirme

SPAM göndericilerinin masraf olarak görebilecekleri temel iki unsur işlemci gücü ve bant genişliği ücretleridir. Günde milyonlarca e-posta gönderen SPAM göndericiler bu yükü kaldıracak bilgisayarlara ve yüksek kapasiteli bant genişliklerine ihtiyaç duyarlar. Ancak SPAM gönderim işini tek merkezden yapmak hem maliyetli hem de tespiti kolaylaştıran bir yöntemdir. Bu nedenle, virüs ve trojan gibi kötü amaçlı yazılımlar sayesinde dünya genelinde binlerce bilgisayarı yönetebilen SPAM göndericileri, zombiye dönüşen bu bilgisayarları kendi amaçları doğrultusunda yönlendirerek, hem bilgisayar gücü hem de bant genişliği anlamında maliyet sorununu ortadan kaldırmaktadırlar.

SPAM gönderim maliyeti bu şekilde sıfırlanabildiğine göre, e-posta göndermenin başka bir yöntemle maliyetlendirilmesi gerekir. Buna cevap olarak ortaya atılan çözüm, e-posta göndermenin ücretli hale getirilmesidir. Ancak ilk akla gelen bu ücretin ne kadar olacağıdır. Normal e-posta kullanıcılarının mağdur olmaması için bu ücretin çok küçük bir miktar olması gerekir. Öyle ki, günde 50-100 e-posta gönderimi yapan bir kişi için rahatsız edici olmayacak bir tutar iken, milyonlarca e-posta gönderen kişiyi caydıracak bir ücretlendirme gerekir. Ayrıca bu ücretleri kimin toplayacağı, hangi yasal çerçeve

dahilinde bu ücretlendirmenin yapılacağı çözülmesi gereken konulardır. Bu öneri kapsamında, normal e-posta kullanıcısını daha az mağdur etmek için, alıcının e-postayı aldığında SPAM veya değil olarak işaretlemesi ve eğer SPAM değil ise bir ücretlendirme yapılmaması da çözümün bir aşaması olabilir. Temel amaç, SPAM göndericisinin bu maliyeti göz önünde bulundurarak SPAM gönderiminden vazgeçmesini sağlamaktır. [22]

4.14. E-posta Gönderiminin Zorlaştırılması

Güçlü bilgisayarlar ve yüksek bağlantı hızları sayesinde, saniyede binlerce e-posta göndermenin mümkün hale gelmesi, SPAM e-posta gönderimini de cazip hale getirmektedir. SPAM e-postaların engellenmesi için, e-posta gönderme sürecine bazı ek işlemler uygulanarak toplu e-posta gönderimleri engellenebilir.

4.14.1. Penny Black Projesi

Projeye adını veren Penny Black pulunun tanıtımı, 1830'lu yıllarda İngiliz Postacılık sistemi reformunda önemli bir rol oynamıştır. Bu dönem öncesinde, postacılık ücretlerinde ağırlık ve mesafe faktörleri baz alınmaktaydı. Her mektup için ayrı hesaplama yapılmaktaydı ve tipik olarak alıcı muhatap tarafından ödeme işlemi gerçekleştirilmekteydi. Penny Black uygulamasının tanıtımıyla birlikte postalama ücret maliyeti postalayan şahsa geçmiş olup, postalama maliyeti hesaplamasındaki karmaşa, standart düşük bir ücret karşılığında giderilmiştir. [39]

Microsoft'un bir girişimi olarak duyurulan, öncesinde de akademik çalışmaların bulunduğu 'Penny Black' projesi, e-posta göndericisini bir bedel ödemeye zorlamak suretiyle SPAM e-postaları azaltmak için bazı teknikler araştırmaktadır. Bu bedel, ilk akla geldiği gibi para şeklinde değil, CPU ve hafıza gibi bilgisayar işlem gücü olarak ödenecektir.

Bu yaklaşım temel olarak, alıcının, e-posta göndericisini tanımadığı durumlarda, göndericinin e-postayı göndermek için bir çaba sarf ettiğini kanıtlaması üzerine kurulmuştur. Örneğin bir bilgisayar işlemcisinin saniyede 10 e-posta gönderdiğini varsayarsak, günde 864.000 e-posta gönderimi yapılır. İşlemci her e-posta gönderimi için 10 saniyelik bir işleme tabi tutulursa, bir bilgisayar için günlük e-posta gönderim limiti

86.400'a düşecektir. Bir e-posta gönderimi için fark edilemeyecek kadar küçük olan bu işlem sayesinde, SPAM e-posta göndericileri yüksek miktarda e-posta gönderebilmek için yüklü bir yatırım yapmak zorunda kalacaklardır. [39] E-posta gönderim süresinin uzatılması, her e-postanın kriptografik bir işlemden geçirilmesi ya da her gönderim için edinilmiş biletlerin alıcı tarafından onaylanması şeklinde olabilir. Bu tip yapılarda e-posta alıcıları, önceden bildikleri ve güvendikleri göndericileri güvenli listelerine alabileceklerdir.

4.14.2. Hashing Algoritmaları

SPAM gönderimini güçleştirmek amacıyla uygulanabilecek bir başka yöntem de, gönderilecek e-postanın, örneğin 5 saniye süren, bir algoritmadan geçmesidir. Her bir e-postaya uygulanan bu fonksiyon, toplu e-posta gönderimlerinin çok uzun süre almasına sebep olacaktır. Normal e-posta kullanıcısı, göndereceği e-postanın beş saniye gecikmesinden mağdur olmayacaktır. Ancak bir seferde on milyon e-posta gönderen SPAM göndericinin işi yaklaşık 600 gün sürecektir. Bu algoritmanın e-posta alıcı tarafında ise hızlı çözülebilmesi gerekir. Hedef e-posta gönderimini yavaşlatmaktır. Alıcının bu yöntemden asgari düzeyde etkilenmesi gerekir.[22]

4.14.3. Spamd

Spamd, OpenBSD projesi tarafından geliştirilmiş bir SPAM erteleme yazılımıdır. Spamd, SPAM göndericilerin yönetimindeki sistemlerden gelen SPAM e-postaları engellemek için etkin bir yöntemdir. SPEWS (Spam Prevention Early Warning System) veritabanında tutulan open relay IP adres listeleriyle yada diğer blacklist IP listeleri kullanılarak SPAM göndericileri engellemek mümkün olabildiği gibi aynı zamanda da SPAM e-posta alımını ciddi ölçüde yavaşlatan bazı özellikleri de bünyesinde barındırmaktadır. Greylisting bileşeni sayesinde belirli bir periyot dahilinde en az bir kez daha teslim edilmek üzere otomatik olarak e-postayı ertelemektedir.[40]

Spews.org adresindeki veritabanına kayıtlı SPAM göndericilerden gelen SMTP trafiği, Spamd yazılımına yönlendirilmektedir. Spamd, kendisine gelen SMTP trafiğini gerçek bir SMTP sunucusu gibi karşılar ve e-postanın gövdesi gönderilmeden önceki tüm adımlarda oldukça yavaş davranarak sunucunun hızını keser. Sıra e-postanın gövdesini göndermeye

geldiğinde ise RFC 821'de belirtilen geçici hata durumlarını ifade eden hata kodlarından birisi ile geri çevrilir. Open relay e-posta sunucusu belirli bir süre sonra gönderimi tekrar deneyerek sürekli aynı sonuç ile karşılaşacaktır. Bu sayede SPAM kaynağı sunucunun kuyruğundaki e-posta sayısı hiç azalmadan sürekli artacak ve open relay sunucu asıl hizmet vermesi gereken yerlere de hizmet veremez duruma gelecektir. Böylece SPAM gönderici gönderemediği SPAM e-posta için çok uzun bir zaman harcayacağı gibi aynı zamanda open relay sistem yöneticisi de artık istese de istemese de SPAM sorununa bir çözüm bulmak zorunda kalacaktır.[41]

4.14.4. CAPTCHA Kullanımı

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) görselleri, yeni nesil Turing testleri olarak kabul edilebilir. Sadece insan gözüyle ve algısıyla, bir resmin içine gömülmüş karakterlerin anlaşılması gerekir. İyi bir CAPTCHA görselinin, resim işleme ve optik karakter tanıma algoritmalarıyla çözülememesi gerekir. E-posta kullanıcısı, göndereceği e-postayı hazırlayıp gönder düğmesine bastığında, karşısına bir CAPTCHA görseli çıkar. Bu CAPTCHA çözüldüğünde e-posta gönderilir. Toplu e-posta gönderimi sırasında sürekli CAPTCHA çözülmesi gerekeceğinden, işin otomatikleştirilmesi mümkün olmaz. Normal e-posta kullanıcıları ise göndereceği her e-posta için yaklaşık 10 saniyelik bir CAPTCHA çözme sürecine maruz kalır. Bu yöntemin getirileri olduğu gibi, vakit kaybı olarak dezavantajları da vardır. [22]

4.15. IPv6

Yeni nesil İnternet Protokolü olan IPv6, 1995 yılında RFC-1883 ile tanımlanmış ve standartlaştırılmıştır. Bu yeni protokolle; adres aralığı sorunu, gerçek zamanlı uygulamalar için daha iyi desteğin sunulması, OSI referans modeline göre 3. katman düzeyinde güvenlik desteğinin sağlanması gibi bazı önemli konularda çözüm sunulmuştur. IPv6'nın IPSec (Internet Protocol Security) desteğiyle birlikte uygulamaya geçirilmesiyle birlikte, günümüzde İnternet ortamında karşılaşılan genel saldırıların önlenmesinin, IPSec protokolünün imkan sağladığı ölçüde olacağı beklenmektedir.[42]

IPSec; IP adreslerinin taklit edilmesi, veri paketlerinin değiştirilmesi ve gizliliğin ihlal edilerek veri trafiğinin izlenmesi gibi sorunlara çözüm sunmak için oluşturulan bir protokoldür.

Günümüzde en sık kullanılan saldırılardan birisi olan ve "IP spoofing" olarak adlandırılan sahte adres kullanma işlemidir. Bu basitçe bir kullanıcının kendi adresini gizlemesi olarak düşünülebilir; fakat diğer taraftan hedefteki kullanıcı aldığı veri paketlerine karşılık yolladığı cevap paketlerini bu sahte adreslere göndereceği için bunu masum bir adres gizleme olarak düşünmek yanlış olacaktır. Bu yöntem SPAM e-posta, DoS, worm ve virüs ataklarında kullanılmaktadır.[42]

IPSec desteğinin aktif bir şekilde yeni nesil IPv6 protokolde kullanılması, kesin güvenlik sağlamamakla birlikte, optimum bir güvenlik seviyesinin sağlanmasını gerçekleştirebilecektir. Sahte IP adresi kullanılarak paket iletiminin engellenmesine yönelik RFC-2827'de çözüm önerisi sunulmuştur. Bu yönteme göre ISP'lerin hizmet sundukları alt ağlar içerisinden gelen paketlerde IP adresi ve altağ maskesi kullanarak ağ kimliğini kontrol edilmesi gerekmektedir.[42]

5. KURUMSAL SUNUCUDAKİ UYGULAMASI

SPAM e-postaların neden olduğu zaman ve iş gücü kaybı ile sistem kaynaklarının kullanımını en aza indirmek için alınabilecek önlemlerin uygulanmasında, e-posta sunucularını kendi bünyesinde barındıran kurumsal şirketlere ve e-posta hizmeti veren kurumlara çok daha fazla görev düşmektedir.

Bu uygulama e-posta sunucusunu kendi bünyesinde barındıran kurumsal bir şirkette gerçekleştirilmiştir. Uygulamanın yeni alınan bir alan adı ile yapılmak yerine, yıllardır aktif olarak kullanılan ve çok sayıda SPAM e-postaya maruz kalan bir alan adı ile yapılması, ortaya çıkacak istatistiki bilgi ve sonuçları verimli kılacaktır.

Uygulama öncesinde sunucudaki tüm SPAM e-posta engelleme yöntemleri kaldırılarak, tüm SPAM e-postaların sunucu ve kullanıcılara ulaşması sağlanmıştır.

5.1. Mevcut Durum

- İşletim Sistemi olarak IBM xSeries206 (Pentium(R) 4 CPU 2.80 Ghz, 2 GB Ram, 73 GB HDD) üzerine Fedora Core 2 linux kuruludur.

- E-posta sunucusu olarak, düşük kaynak tüketimi, yüksek performansı ve açık kaynak kodlu olması sebebiyle Qmail kullanılmaktadır.

- Qmail e-posta sunucusunda 82 e-posta hesabı kullanılmaktadır.

- E-posta sunucusunun logları takip edilmekte ve tüm kullanıcılar günlük ortalama 6.900 e-posta almaktadır.

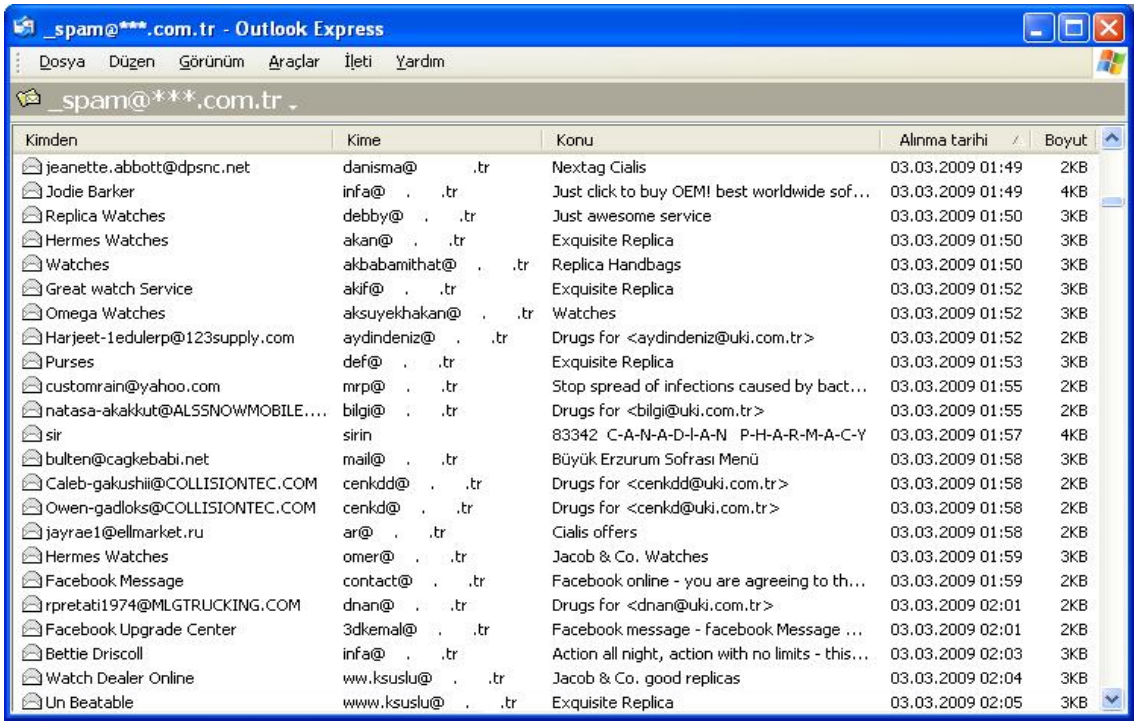
- Kurumsal şirketlerde en sık kullanılan ve dolayısıyla SPAM göndericilerin hedefi haline gelen info hesabı takip edilmekte ve günlük ortalama 175 e-posta alınmaktadır. Bu e-postaların ortalama 159 adedi SPAM e-postalardan oluşmaktadır.

- Genel ortalamaya yakın olan bir kullanıcının e-posta hesabı takip edilmekte ve günlük ortalama 65 e-posta alınmaktadır. Bu e-postaların ortalama 62 adedi SPAM e-postalardan oluşmaktadır.

Günlük Ortalama	info@...	kemal@...	Toplam
SPAM E-Posta Miktarı	159	62	221
Normal E-Posta Miktarı	20	3	23
Toplam E-posta Miktarı	179	65	244
SPAM E-Posta Oranı	89%	95%	91%

Şekil 26 - Kurumsal Sunucudaki Kullanıcıların Ortalama SPAM E-Posta Yoğunlukları

- Sözlük saldırılarının takip edilmesi açısından önemli olan CatchAll(*) hesabı takip edilmekte ve günlük ortalama 7.650 e-posta alınmaktadır ve tamamı SPAM e-postalardan oluşmaktadır. spam@xxx.com.tr, CatchAll hesabı olarak ayarlanmıştır.



Şekil 27 – CatchAll Hesabındaki Sözlük Saldırıları

CatchAll hesabındaki durumdan anlaşılacağı gibi sözlük saldırıları, sunucuya ulaşan günlük ortalama 14.500 e-postanın yüzde 53'lük kısmını oluşturmaktadır. Her ne kadar CatchAll hesabına gelen e-postalar kullanıcılara ulaşmıyor olsa da, e-posta sunucusunda oluşturduğu yük ve trafik açısından engellenmesi oldukça önemlidir.

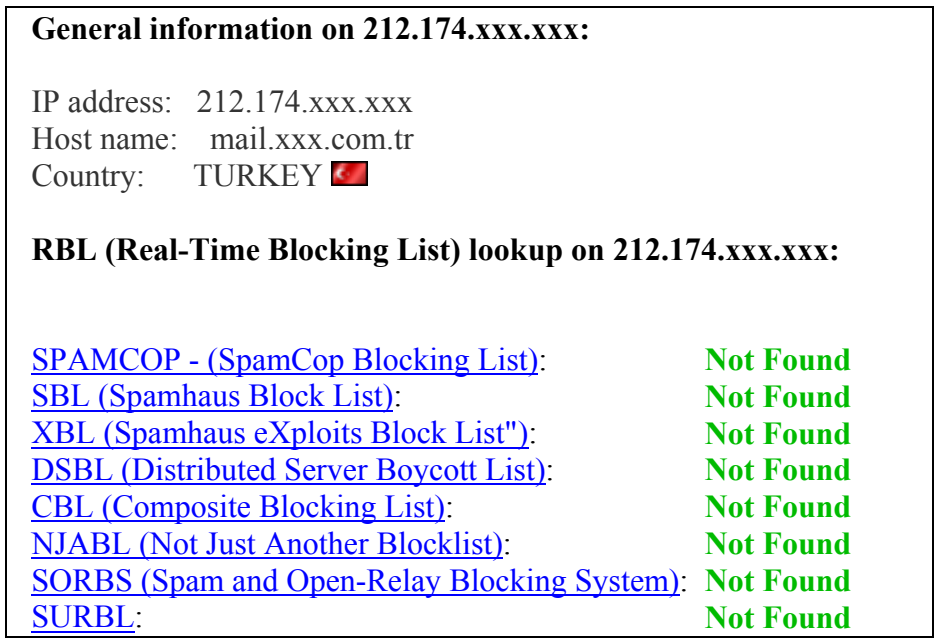
(*) CatchAll hesabı, sunucuda var olmayan kullanıcı hesaplarına gönderilen e-postaları yakalamak için kullanılmaktadır.

- Sunucunun Relay ve ters DNS kayıtları düzgün bir şekilde yapılandırılmıştır.

RESULT: 212.174.xxx.xxx	
Banner:	220 mail.xxx.com.tr ESMTP
Connect Time:	0 seconds – Good
Transaction Time:	0.844 seconds – Good
Relay Check:	OK - This server is not an open relay.
Rev DNS Check:	OK - 212.174.xxx.xxx resolves to mail.xxx.com.tr
GeoCode Info:	Geocoding server is unavailable
Session Transcript:	HELO please-read-policy.mxtoolbox.com 250 mail.xxx.com. [312 ms] MAIL FROM: <test@mxtoolbox.com> 250 [359 ms] RCPT TO: <test@mxtoolbox.com> 553 sorry, that domain isn't in my list of allowed rcpthosts (#5.7. [281 ms] QUIT 221 mail.xxx.com. [359 ms]

Şekil 28 - Sunucunun Relay ve ters DNS kayıtlarının durumu
http://www.mxtoolbox.com/diagnostic.aspx

- Sunucu herhangi bir RBL karalistesinde yer almamaktadır.



General information on 212.174.xxx.xxx:

IP address: 212.174.xxx.xxx
Host name: mail.xxx.com.tr
Country: TURKEY

RBL (Real-Time Blocking List) lookup on 212.174.xxx.xxx:

SPAMCOP - (SpamCop Blocking List):	**Not Found**
SBL (Spamhaus Block List):	**Not Found**
XBL (Spamhaus eXploits Block List"):	**Not Found**
DSBL (Distributed Server Boycott List):	**Not Found**
CBL (Composite Blocking List):	**Not Found**
NJABL (Not Just Another Blocklist):	**Not Found**
SORBS (Spam and Open-Relay Blocking System):	**Not Found**
SURBL:	**Not Found**

Şekil 29 - Sunucunun RBL listelerindeki durumu
http://www.ipchecking.com/

5.2. Yöntemlerin Kurumsal Sunucuda Uygulanması

Bölüm 4'te anlatılan tüm SPAM engelleme yöntemlerinin bir arada kullanılması mümkün olmadığından, kurumsal sunucunun yapısına ve performansına uygun açık kaynak kodlu yöntemler seçilmiştir. Uygulama, yöntemlerin ayrı ayrı değerlendirilebilmesi açısından aynı anda değil, kullanılan tekniklere göre 1 ay içerisinde 5'er günlük periyotlar halinde uygulanmıştır.

- Clamav Antivirus / 01.03.09 – 05.03.09
- Spamassassin Required_Hits 10 / 06.03.09 – 10.03.09
- Spamassassin Required_Hits 3 + Bayes Auto Learn / 11.03.09 – 15.03.09
- Razor / 16.03.09 – 20.03.09
- Pyzor / 16.03.09 – 20.03.09
- DCC / 16.03.09 – 20.03.09
- RBL (Gerçek Zamanlı Karaliste) / 21.03.09 – 25.03.09
- Tarpit Patch / 26.03.09 – 31.03.09

5.2.1. Clamav Antivirus Kurulumu

Kurulum için *http://www.clamav.net/binary.html* adresinden son sürüm indirilir. Kuruluma geçmeden önce

groupadd clamav

useradd -g clamav -s /bin/false -c “Clamav Antivirus” clamav

komutlarıyla clamav kullanıcısı ve grubu oluşturulur.

tar -zxvf clamav-0.x.tar.gz

./configure --prefix=/usr/local/ -without-libcurl

make

make install

komutlarıyla kurulum tamamlanır. Clamd yapılandırması “/usr/local/etc/clamd.conf” dosyasında yapılır. Yapılandırma yapılırken ‘ LogFile /var/log/clamd.log’, ‘DatabaseDirectory /usr/local/share/clamav ‘ ve ‘ User clamav ‘ değişkenleri verilmelidir. Clamav “/etc/init.d/clamd start” ile başlatılır.

Clamav ile manuel olarak virüs taraması yapmak için clamdscan komutu kullanılır. Örneğin /home dizinini virüs taraması yapmak için, “clamdscan /home --move=/karantina -v --stdout” komutu kullanılır. Bu komutla, bulunan virüslü dosyaların --move ile /karantina dizinine taşınması ve -v --stdout ile işlem sonucunun detaylı görüntülenmesi sağlanmıştır.

5.2.1.1. Clamav Veritabanının Güncellenmesi

Clamd hizmetinin başlatılmasıyla birlikte antivirus veritabanını güncel tutmak için görevli olan freshclam hizmeti de başlatılır.

Freshclam yapılandırması “/etc/freshclam.conf” dosyasında yapılır. Burada güncelleme için veritabanı yolu ‘DatabaseDirectory /usr/local/share/clamav ‘ şeklinde belirtilmelidir. Yapılandırma dosyasında freshclam hizmeti varsayılan olarak her saat başı İnternetten güncelleme yapılıp yapılmadığına bakar. Eğer güncelleme manuel olarak yapılmak istenirse, komut satırında “freshclam -v” komutu kullanılmalıdır.

5.2.2. Spamassassin Kurulumu

Öncelikle Spamassassin Perl dilinde yazıldığından dolayı sistemde perl kurulu olmalıdır. Kurulum için *http://spamassassin.apache.org/downloads.cgi* adresinden son sürümü indirilir.

spamassassin-3x.tar.bz2
tar -jxvf spamassassin-3x.tar.bz2
perl Makefile.PL
make
su -
make install

komutlarıyla kurulum gerçekleştirilir. Kurulumdan sonra spamassassin'in çalışması, ornek.txt adlı boş bir dosya oluşturarak, "spamassassin -t < ornek.txt > ornek.out" komutuyla test edilebilir.

5.2.2.1 Spamassassin'in Yapılandırılması

Spamassassin'in yapılandırma dosyası olan local.cf dosyası, /etc/mail/spammassassin dizininin altında bulunur. Yapılan ayarlar "spamassassin --lint -D" komutuyla sınanabilir. Bu komut local.cf dosyasındaki kabul edilmeyen girdileri listeler ve -D parametresi ile hata ayıklama yapılabilmesini sağlar.

Kurumsal sunucudaki Spamassassin yapılandırmaları sonrasında ortaya çıkan local.cf dosyası aşağıdaki gibidir.

required_hits 3.0
use_bayes 1
bayes_auto_learn 1
use_razor2 1
use_pyzor 1
use_dcc 1
skip_rbl_checks 0

*blacklist_from *@dal-tech.com*

...

*whitelist_from *@teleweb.com.tr*

…

- *required_hits 3.0*

Bir e-postanın 3.0 puanı aştıktan sonra SPAM olarak değerlendirileceği anlamına gelir. Bu eşik değerin arttırılması SPAM yakalama ihtimalini azalttığı gibi, azaltılması durumunda normal E-postaların yakalanma ihtimalini arttırmaktadır.

- *use_bayes 1, bayes_auto_learn 1*

Bu iki satır Spamassassin'in Bayes öğrenme yöntemi ile ilgili olan satırlardır. Bu yöntem daha önce gelen e-postaları esas alarak, olasılık hesaplarıyla, bir sonraki e-postanın SPAM olup olmadığını tahmin ederek çalışır.

- *skip_rbl_checks 0*

Karaliste kontrolünün yapılması için kullanılır. skip_rbl_checks değeri 1 yapılırsa karaliste (RBL) kontrolü yapılmaz.

- *use_razor2 1, use_pyzor 1, use_dcc 1*

Bu satırlar Spamassassin'in Razor, Pyzor ve DCC uygulamalarıyla bir bütünlük içinde çalışmasını sağlar.

- *blacklist_from *@dal-tech.com*

Bir alan adından gelen tüm e-postaları SPAM olarak işaretlemek için kullanılır.

- *whitelist_from *@teleweb.com.tr*

Bir alan adından gelen tüm e-postaların hiçbir zaman SPAM olarak değerlendirilmemesi için kullanılır.

5.2.2.2. E-Postaların Spamassassin'e Öğretilmesi

Kullanıcılar sa-learn komutunu kullanarak gelen e-postaları sisteme SPAM ya da SPAM değil şeklinde tanıtabilirler. Bu özellik, o zamana kadar Spamassasin'e tanıtılan e-postaları temel alarak, daha sonra gelecek olan e-postaların değerlendirilmesinde yardımcı olur.

Spamassassin'e bir e-postanın SPAM olduğunu bildirmek için sa-learn komutu, "sa-learn --spam "e-postaların_bulunduğu_dizin_veya_dosya" " şeklinde kullanılır. Aynı şekilde bir e-postanın SPAM olmadığını bildirmek için de sa-learn komutu, "sa-learn --ham "e-postaların_bulunduğu_dizin_veya_dosya" " şeklinde kullanılır.

5.2.4. Razor Kurulumu

Kurulum için *http://sourceforge.net/project/showfiles.php?group_id=3978* adresinden razor-agent ve razor-agent-sdk tar paketlerinin son sürümleri indirilir.

Öncelikle,
tar -jxvf razor-agent-sdk-2.xx.tar.bz2
perl Makefile.PL
make
make test
make install
komutlarıyla razor-agent-sdk paketi kurulur, daha sonra da,
tar -jxvf razor-agent-2.xx.tar.bz2
perl Makefile.PL
make
make test
make install
komutlarıyla razor-agent paketi açılıp derlenerek kurulum tamamlanır.

Kurulumdan sonra Razor'un gerekli araçlarına sembolik bağları ataması için, "razor-client", Razor'un gerekli yapılandırma dosyalarını oluşturabilmesi için de "razor-admin -

create” komutu kullanılır. Böylece o anki kullanıcının ev dizininde .razor adlı dizinin altında gerekli dosyaları oluşturulur.

Razor sunucusuna raporlama yapabilmesi için “razor-admin -register -user=kemal -pass=xxx” komutuyla kullanıcı adı ve parola oluşturulur. SPAM e-postaları Razor sunucusuna raporlamak için, “razor-report” , SPAM olmayan normal e-postaları bildirmek için ise “razor-revoke” komutları kullanılır.
Razor'u Spamassassin ile birlikte çalıştırabilmek için /etc/mail/spamassassin/local.cf dosyasına, “use_razor2 1” satırı eklenerek spamassassin yeniden başlatılmalıdır. Razor’un spamassassin ile çalışmasını sınamak için “spamassassin --lint -D” komutunun sonucunda Razor sunucusuna bağlanabildiği görünmelidir.

5.2.5. Pyzor Kurulumu

Kurulum için *http://sourceforge.net/project/showfiles.php?group_id=50000* adresinden son sürümü indirilir.

tar -jxvf pyzor-0.4.x-tar.bz2
python setup.py build
python setup.py install
komutlarıyla kurulur ve aşağıdaki dizinler için gerekli paylaşım izinlerini ayarlanır.
chmod -R a+rX /usr/share/doc/pyzor0.4x
chmod -R a+rX /usr/lib/python2.3/site-packages/pyzor
chmod -R a+rX /usr/bin/pyzor
chmod -R a+rX /usr/bin/pyzord
Komutların kullanımı da Razor'a benzemektedir. Report SPAM e-postalar, Whitelist ise SPAM olmayan e-postalar için kullanılmaktadır.

Pyzor'u Spamassassin ile birlikte çalıştırabilmek için /etc/mail/spamassassin/local.cf dosyasına, “use_pyzor 1” satırı eklenerek spamassassin yeniden başlatılmalıdır. Pyzor’un spamassassin ile çalışmasını sınamak için “spamassassin --lint -D” komutunun sonucunda Pyzor sunucusuna bağlanabildiği görünmelidir.

5.2.6. DCC (Distributed Checksum Clearinghouse) Kurulumu

Kurulum için *http://www.rhyolite.com/anti-spam/dcc/source/dcc.tar.Z* adresinden son sürüm indirilir.

tar -zxvf dcc.tar.Z
./configure --prefix=/usr
make
su -
make install
komutlarıyla kurulum yapıldıktan sonra "cdcc info" komutuyla DCC sunucularına bağlanabilirliği test edilir. Test sonucu, "dcc1.dcc-servers.net,- RTT+0 ms anon" şeklindeyse DCC sunucularına bağlantı sağlanmış demektir.

DCC'yi Spamassassin ile birlikte çalıştırabilmek için /etc/mail/spamassassin/local.cf dosyasına, "use_dcc 1" satırı eklenerek spamassassin yeniden başlatılmalıdır. DCC'nin spamassassin ile çalışmasını sınamak için "spamassassin --lint -D" komutunun sonucunda DCC'nin sunucusuna bağlanabildiği görünmelidir.

5.2.3. RBL (Gerçek Zamanlı Karaliste) Kontrolü

Sisteme eklenmek istenen gerçek zamanlı karalisteler, /var/qmail/supervise/qmail-smtpd dizinindeki "run" dosyasında aşağıdaki şekilde yapılandırılır.
exec /usr/local/bin/softlimit -m 50000000 \
/usr/local/bin/tcpserver -v -R -l "$LOCAL" -x /etc/tcp.smtp.cdb -c "$MAXSMTPD" \
-u "$QMAILDUID" -g "$NOFILESGID" 0 smtp \
/var/qmail/bin/qmail-smtpd mail.uki.com.tr \
/home/vpopmail/bin/vchkpw /bin/true \
/usr/local/bin/rblsmtpd -r bl.spamcop.net -r list.dsbl.org -r safe.dnsbl.sorbs.net -r sbl-xbl.spamhaus.org -r blackholes.njabl.org qmail-smtpd 2>&1

Kurumsal sunucuya spamcop, dsbl, sorbs, spamhaus ve njabl organizasyonlarının gerçek zamanlı karaliste kontrolü eklenmiştir. Yapılan değişikliklerin etkinleşmesi için "Svc -t /var/qmail/supervise/qmail-smtpd" komutuyla servisin yeniden etkinleştirilmesi gerekir.

Gerçek zamanlı karalisteleri Spamassassin ile birlikte çalıştırabilmek için /etc/mail/spamassassin/local.cf dosyasına, "skip_rbl_checks 0" satırı eklenerek spamassassin yeniden başlatılmalıdır.

5.2.7. Tarpit Patch Uygulanması

Qmailde tarpit dosyaları, bir e-posta göndericisinin tek bir seferde belli bir sayıdan fazla kişiye e-posta gönderdiğinde, her bir alıcı adresi için göndericiyi belirli bir süre geciktirmesine olanak sağlar [36]. SMTP aktarımında yapılan bu gecikmeleri sağlamak için, *http://www.palomine.net/qmail/tarpit.html* adresindeki patch'in qmail'in kaynak kodları içinde yer alan qmail-smtpd.c dosyasına uygulanması gerekir.

Patch'in uygulanması için öncelikle patch kodu, qmail kaynak kodlarının bulunduğu /usr/src/qmail-1.x dizininde tarpit.patch dosyası haline getirilir ve bu dizin içerisinde,

```
patch tarpit.patch
patch < tarpit.patch
```

komutlarıyla patch uygulanır. Patch uygulandıktan sonra qmail yeniden derlenerek tarpit patch'inin qmail'de etkinleşmesi sağlanır.

Tarpit yapılandırma dosyaları, /var/qmail/control/ dizininde yer alan "tarpitcount" ve "tarpitdelay" dosyalarıdır. Kurumsal sunucuda, e-postanın tek seferde en az 5 alıcıya gönderilmesi durumunda her alıcı adresi için 20 saniye bekletilmesini sağlamak için "tarpitcount" değerini 5, "tarpitdelay" değerini de 20 olarak ayarlanmıştır. Böylece gönderici 5x20=100 saniye beklemek zorunda kalacaktır.

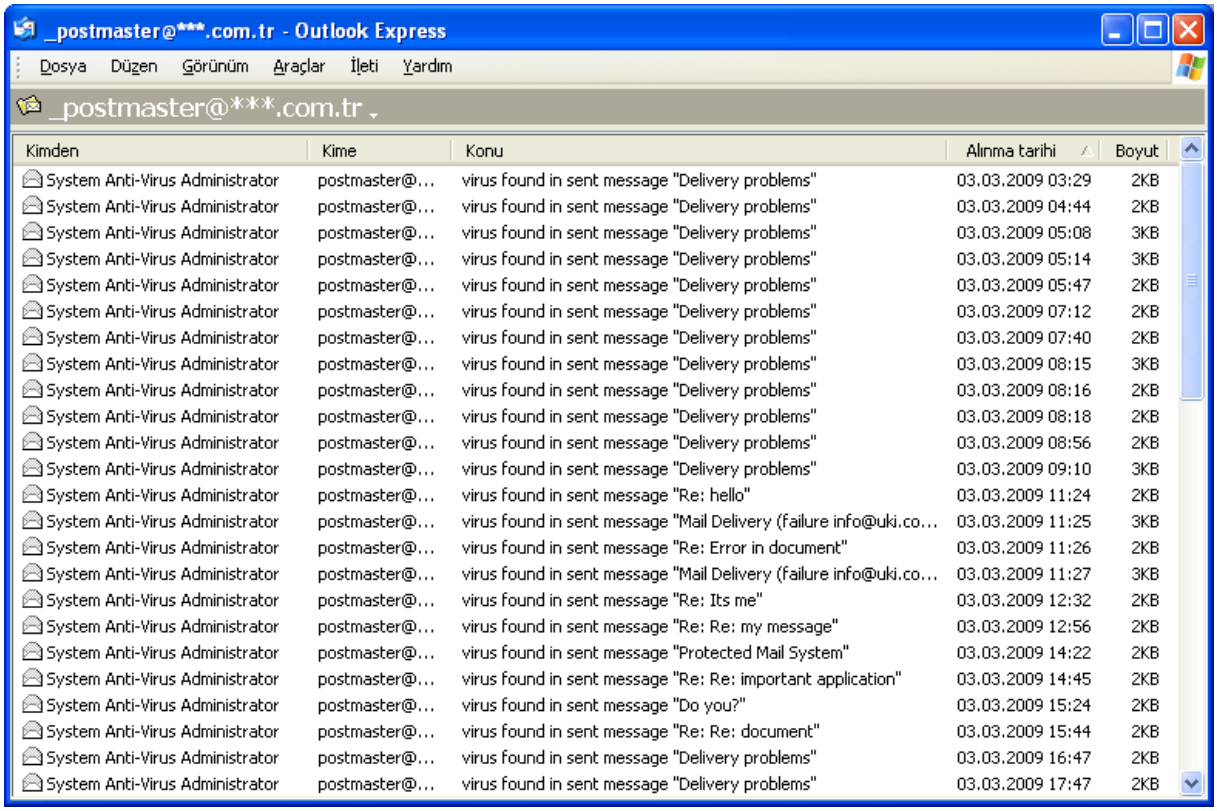
5.3. Uygulama Sonuçları

Kurumsal sunucudaki uygulama, 4 farklı e-posta hesabının takibiyle sağlanan verilerle değerlendirilmiştir. Clamav Antivirüs yazılımıyla yakalanan virüs içerikli e-postaların takibi *postmaster@xxx.com.tr*, sözlük saldırısı şeklinde sunucuya ulaşan SPAM e-postaların takibi *spam@xxx.com.tr*, kullanıcılara ulaşan SPAM e-postaların takibi de *info@xxx.com.tr* ve *kemal@xxx.com.tr* hesaplarıyla yapılmıştır. Sonuçlara ilişkin detaylı veriler Şekil 30'da verilmiştir.

Uygulamalar	*postmaster@xxx.com.tr*		*spam@xxx.com.tr*		*info@xxx.com.tr*		*kemal@xxx.com.tr*	
	Günlük Virüslü E-posta Miktarı	Virüslü E-Posta Azalma Oranı	Günlük SPAM E-posta Miktarı	SPAM E-Posta Azalma Oranı	Günlük SPAM E-posta Miktarı	SPAM E-Posta Azalma Oranı	Günlük SPAM E-posta Miktarı	SPAM E-Posta Azalma Oranı
Uygulama Öncesi	0	-	7.644	-	159	-	62	-
Clamav Antivirüs	85	0%	7.709	0%	161	0%	61	0%
Spamassassin Required Hits 10	70	18%	4.314	44%	87	45%	32	48%
Spamassassin Required Hits 3 + Bayes Auto Learn	41	52%	2.636	66%	49	69%	17	72%
razor + pyzor + DCC	21	75%	2.161	72%	41	75%	13	79%
RBL Kontrolü	18	79%	1.742	77%	32	80%	10	84%
Tarpit Patch	19	78%	1.191	84%	29	82%	8	87%

Şekil 30 – Uygulamaların Sunucudaki SPAM E-Posta Trafiğine Etkisi

Kurumsal sunucuya ilk uygulanan yöntem olan Clamav antivirüs yazılımının yakaladığı virüs içerikli e-posta bilgileri postmaster hesabına yönlendirilerek takibi bu hesapta yapılmaktadır. Clamav antivirüs yazılımının sunucuda devreye girmesiyle birlikte ilk 5 günlük dönem için postmaster hesabına günde ortalama 85 e-postanın virüs içerikli e-posta bilgisinin ulaştığı görülmüştür. Böylece virüslü bu e-postaların kullanıcılara ulaşmadan silinmesi sağlanmıştır. Şekil 31'de postmaster hesabına ulaşan virüs içerikli e-posta bilgisi verilmiştir.



Kimden	Kime	Konu	Alınma tarihi	Boyut
System Anti-Virus Administrator	postmaster@...	virus found in sent message "Delivery problems"	03.03.2009 03:29	2KB
System Anti-Virus Administrator	postmaster@...	virus found in sent message "Delivery problems"	03.03.2009 04:44	2KB
System Anti-Virus Administrator	postmaster@...	virus found in sent message "Delivery problems"	03.03.2009 05:08	3KB
System Anti-Virus Administrator	postmaster@...	virus found in sent message "Delivery problems"	03.03.2009 05:14	3KB
System Anti-Virus Administrator	postmaster@...	virus found in sent message "Delivery problems"	03.03.2009 05:47	2KB
System Anti-Virus Administrator	postmaster@...	virus found in sent message "Delivery problems"	03.03.2009 07:12	2KB
System Anti-Virus Administrator	postmaster@...	virus found in sent message "Delivery problems"	03.03.2009 07:40	2KB
System Anti-Virus Administrator	postmaster@...	virus found in sent message "Delivery problems"	03.03.2009 08:15	3KB
System Anti-Virus Administrator	postmaster@...	virus found in sent message "Delivery problems"	03.03.2009 08:16	2KB
System Anti-Virus Administrator	postmaster@...	virus found in sent message "Delivery problems"	03.03.2009 08:18	2KB
System Anti-Virus Administrator	postmaster@...	virus found in sent message "Delivery problems"	03.03.2009 08:56	2KB
System Anti-Virus Administrator	postmaster@...	virus found in sent message "Delivery problems"	03.03.2009 09:10	3KB
System Anti-Virus Administrator	postmaster@...	virus found in sent message "Re: hello"	03.03.2009 11:24	2KB
System Anti-Virus Administrator	postmaster@...	virus found in sent message "Mail Delivery (failure info@uki.co...	03.03.2009 11:25	3KB
System Anti-Virus Administrator	postmaster@...	virus found in sent message "Re: Error in document"	03.03.2009 11:26	2KB
System Anti-Virus Administrator	postmaster@...	virus found in sent message "Mail Delivery (failure info@uki.co...	03.03.2009 11:27	3KB
System Anti-Virus Administrator	postmaster@...	virus found in sent message "Re: Its me"	03.03.2009 12:32	2KB
System Anti-Virus Administrator	postmaster@...	virus found in sent message "Re: Re: my message"	03.03.2009 12:56	2KB
System Anti-Virus Administrator	postmaster@...	virus found in sent message "Protected Mail System"	03.03.2009 14:22	2KB
System Anti-Virus Administrator	postmaster@...	virus found in sent message "Re: Re: important application"	03.03.2009 14:45	2KB
System Anti-Virus Administrator	postmaster@...	virus found in sent message "Do you?"	03.03.2009 15:24	2KB
System Anti-Virus Administrator	postmaster@...	virus found in sent message "Re: Re: document"	03.03.2009 15:44	2KB
System Anti-Virus Administrator	postmaster@...	virus found in sent message "Delivery problems"	03.03.2009 16:47	2KB
System Anti-Virus Administrator	postmaster@...	virus found in sent message "Delivery problems"	03.03.2009 17:47	2KB

Şekil 31 – Postmaster Hesabındaki Virüs İçerikli E-Posta Bilgileri

İkinci 5 günlük dönemde kurulan Spamassassin, eşik değeri(Required Hits) 10 olarak yapılandırılmış olmasına rağmen SPAM e-postaları, ortalama yüzde 45 gibi önemli bir oranda engellemiştir.

Sonraki 5 günlük dönemde Spamassassin yeniden yapılandırılmış ve Bayes'in otomatik öğrenme özelliği etkinleştirilerek, eşik değeri 3 olarak ayarlanmıştır. Spamassassin bu haliyle, sözlük saldırısı şeklindeki SPAM e-postaların engellenme oranını yüzde 66'ya

yükseltirken, kullanıcılara ulaşan SPAM e-postaların engellenme oranını yüzde 70'e kadar yükseltmiştir.

SPAM e-posta imza depoları olarak kullanılan Razor, Pyzor ve DCC kurulumlarının yapıldığı sonraki 5 günlük dönemde, sözlük saldırısı şeklindeki SPAM e-postaların engellenme oranı yüzde 72'ye, kullanıcılara ulaşan SPAM e-postaların engellenme oranını da ortalama yüzde 76'ya yükselmiştir.

Sonraki 5 günlük dönemde ise Spamcop, Dsbl, Sorbs, SpamHaus ve Njabl RBL kontrolleri sisteme eklenmiştir. RBL kontrollerinin devreye girmesiyle SPAM e-posta engelleme oranı yüzde 81'lere kadar ulaşmıştır.

Son olarak uygulanan yöntem olan Tarpit patch uygulamasıyla, sözlük saldırısı şeklindeki SPAM e-postaların engellenme oranı yüzde 7'lik bir artışla yüzde 84'e ulaşmıştır. Kullanıcılara ulaşan SPAM e-postaların engellenme oranı ise bu artışın çok altında kalarak ortalama yüzde 81'den yüzde 83 seviyesine ancak ulaşabilmiştir.

Uygulama sonuçlarında dikkat çeken bir başka nokta ise, SPAM engelleme oranı yükseldikçe virüs içerikli e-postalarda yaşanan düşüştür. Clamav antivirüs kurulumuyla günde ortalama 85 virüs içerikli e-posta yakalanırken, SPAM engelleme yöntemlerinin devreye girmesiyle yaklaşık yüzde 78'lik bir düşüşle günde 19 e-postaya kadar gerilemiştir. Bu durum virüslü içeriğin SPAM e-postalarla taşındığının ve/veya virüs içerikli e-postaların SPAM e-postalarla benzer yapıda olduklarının önemli bir göstergesidir.

6. SONUÇ ve ÖNERİLER

Günümüzde SPAM e-postaların engellenmesine yönelik kullanılan yöntemlerle SPAM e-postaların sunuculara, hatta kullanıcılara kadar ulaşması kaçınılmazdır. SPAM e-postaların sunucuya kadar ulaşması her ne kadar İnternet omurgasındaki trafiğin önemli bir kısmını oluşturmuş olsa da, sunucu ve kullanıcı tarafında alınabilecek önlemlerle SPAM e-postaların son kullanıcılara ulaşmasını önleyerek, harcanan saklama alanını, vakit ve iş gücü kaybını en aza indirmek mümkündür. Ayrıca alınacak bu önlemlerle, SPAM e-posta trafiğinin en önemli nedeni olan botnetlerin oluşmasını sağlayan kötü amaçlı yazılım içerikli SPAM e-postaların yayılması da önemli ölçüde engellenebilecektir.

Bu çalışmada kurumsal sunucuda uygulanan yöntemlerle, SPAM e-posta trafiğinin ortalama yüzde 83'lük bölümü engellenmiştir. Sistemin takip edilerek yapılandırılması, belirli bir süre SPAM e-postaların sunucuya bildirilmesi ve Spamassassin'in Bayes öğrenme özelliği sayesinde bu oranın zamanla artması beklenmektedir. Sistemin bütünlüğünü sağlamak için sunucuda uygulanan bu yöntemler, kullanıcı tarafında uygulanacak yöntemlerle desteklenmelidir. Bu amaçla yapılan diğer bir çalışmada, bir kullanıcıya aynı dönem içerisinde ulaşan e-postaların hem "Microsoft Office Outlook 2003 (SP3)" hem de Mozilla Thunderbird (sürüm 2.0.0.17 / Gereksiz Posta Ayarı: SpamAssassin) e-posta istemcileriyle alınması sağlanmıştır. Microsoft Office Outlook 2003 SPAM e-postaların yüzde 71'ini, Mozilla Thunderbird ise yüzde 69'unu engellemiştir. Her ikisinin de öğrenebilir yapıda olması SPAM e-posta engelleme oranını arttıracağı gibi, zamanla kullanıcılara göre karar vermesine olanak sağlayacağından SPAM tanımının esnekliğini de ortadan kaldıracaktır.

Sunucu ve kullanıcı tarafında günümüzde uygulanan yöntemlerle kullanıcılara ulaşan SPAM e-postaları tümüyle engellemek mümkün olsa dahi, SPAM e-posta trafiği zaten oluşmuş olacaktır. İnternet omurgasındaki SPAM e-posta trafiğini ve harcanan bant genişliğini tümüyle ortadan kaldırmak, ancak SMTP aktarımından önce alınabilecek caydırıcı yöntemlerle ya da SMTP aktarımı sırasında uygulanabilecek yöntemlerle mümkün olabilir. Şu anki sistemle e-posta göndermek, PTT şubelerinden mektup göndermeye benzemektedir. Örneğin şu anki durumda, İstanbul'da ikamet eden A,

Antalya'da ikamet eden B'ye istediği bir PTT şubesinden, "Gönderen" kısmına farklı bir C ismi ve adresi yazarak herhangi bir kimlik kontrolü olmaksızın mektup gönderebilmektedir. Bu durumda gönderilen mektup Antalya'daki B alıcısının posta kutusuna kadar ulaşmaktadır. B, mektubu okumadan yırtıp atsa dahi, mektup PTT şubelerinde ve alıcının posta kutusunda bir yer işgal ederek İstanbul ile Antalya arasında bir trafik oluşturmuştur. Bu durumun önüne geçebilmek için A'nın sadece ikamet ettiği İstanbul'daki PTT şubesinden kimlik ve adres kontrolü yapıldıktan sonra mektup gönderebilmesi gerekir.

E-posta sisteminde bunu sağlamak, kullanıcıların kendi alan adları ile sadece kendi sunucuları tarafından e-posta göndermesiyle mümkün olabilir. Her ne kadar Relay, ters DNS ve SPF kaydı gibi yöntemlerle bunu sağlamak mümkün olsa da bu kayıtların tüm sunucular tarafından kullanılmaması nedeniyle tümüyle işlerlik kazanamamaktadır. Bu duruma bütünsel olarak işlerlik kazandırmak için alan adlarının e-posta kullanımında MX, DNS, Relay ve ters DNS gibi kayıtların uygunluğundan oluşacak kriterler belirlenebilir. Resmi bir kurum tarafından belirlenecek ve kontrol edilecek olan kriterlerin uygunluğu halinde ilgili alan adına, içinde kullanım süresi ve günlük kota gibi bilgilerin de yer alabileceği bir onay sertifikası verilerek e-posta kullanımının bu sertifika ile yapılması sağlanabilir. Sistemin sürekliliği açısından bu kriterlerin zorunlu hale getirilmesi, düzenli olarak denetlenmesi ve kriterlerin dışına çıkılması durumunda da e-posta hizmetinin durdurulması gibi yaptırımlar sağlanabilir.

Kaynakça

[1] Postel, J.B., "Simple Mail Transfer Protokol", RFC 821, August 1982.

[2] Freed, N., Borenstein, N., "Multipurpose Internet Mail Extensions", RFC 2045, November 1996.

[5] Alataş, Ş., "SMTP Sorununa Yeni Bir Yaklaşım: Sistemin Yeniden İnşası" Akademik Bilişim Konferansı, Denizli, 2006

[10] IBM Internet Security Systems X-Force® 2008 Trend & Risk Report
IBM Global Technology Services, January 2009

[11] MessageLabs Intelligence: 2008 Annual Security Report
MessageLabs | Now part of Symantec™, January 2009

[12] The State of Spam A Monthly Report, Generated by Symantec Messaging and Web Security, February 2009.

[13] Cisco 2008 Annual Security Report,
Updated with complete 2008 data, February 2009.

[22] Gündüz, H.C., "SPAM 2.0, Tespit ve Engelleme Yöntemleri",
Akademik Bilişim Konferansı, Kütahya, 2007

[23] Yan, G., Ming Y., Xiaonan Z., Pardo, B., Ying W., Pappas, T.N.; Choudhary, A., "Image SPAM hunter", Acoustics, Speech and Signal Processing 2008, ICASSP 2008, IEEE International Conference on March-April 2008, s:1765 – 1768.

[24] Sandford, PJ., Sandford, JM., Parish, DJ., "Analysis of SMTP Connection Characteristics for Detecting SPAM Relays", Computing in the Global Information Technology 2006, ICCGI '06, International Multi-Conference on Aug. 2006, s:68 – 68.

[29] Altunyaprak, C., "Bayes Yöntemi Kullanarak İstenmeyen Elektronik Postaların Filtrelenmesi", Muğla Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 2006.

[30] Wong, M., Schlitt, W., "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1", RFC 4408, April 2006.

[33] Çağrı Yücel. Koç Üniversitesi. Alternatif bir araç olarak Spamassassin
http://www.ulakbim.gov.tr/dokumanlar/guvenlik/Cagri_Yucel.pdf

[34] Karabatak, G., Türk, M., Türkoğlu, İ., "Çöp E-Postaları Engelleme Sistemi Geliştirme" Fırat Üniv. Fen ve Müh. Bil. Dergisi, 2008.

[35] Yang, L., Bin-Xing, F., Li, G., Zhi-Hong T., Yong-Zheng Z., Zhi-Gang W., "UBSF: A novel online URL-Based SPAM Filter" Computers and Communications 2008, ISCC 2008, IEEE Symposium on July 2008, s:332 – 339.

[36] Yenigül, İ., Şimşek B., Önal H., "qmail Yüksek Performanslı E-Posta Sunucu" Açık Akademi, 2005.

[37] Çıtlık, A., "Time Efficient SPAM E-Mail Filtering for Turkish", Graduate Program in Computer Engineering, Bogaziçi University, 2006.

[38] Dhinakaran, C., Jae K.L., Nagamalai, D., "Characterizing SPAM Traffic and Spammers" Convergence Information Technology, 2007. International Conference on Nov. 2007, s:831 – 836.

[39] Microsoft. Penny Black. http://research.microsoft.com/research/sv/PennyBlack/

[42] Efe, A., "Yeni Nesil İnternet Protokülü'ne(IPv6) Geçişle Birlikte İnternet Saldırılarının Geleceğine Yönelik Beklentiler", Akademik Bilişim Konferansı, Denizli, 2006.

İnternet Kaynakçası

[3] E-mail. http://en.wikipedia.org/wiki/E-mail

[4] Ethem Evlice, "SMTP Server Kullanmadan E-posta Gönderme (.NET)" http://www.csharpnedir.com/makalegoster.asp?MId=119

[7] DNS. http://tr.wikipedia.org/wiki/DNS

[8] http://www.spam.org.tr

[9] Yığın İleti. http://tr.wikipedia.org/wiki/SPAM

[14] http://www.marshal.com

[15] Phishing Statistics from TRACE :: Marshal,
Statistics for Week ending March 15, 2009.
http://www.marshal.com/TRACE/phishing_statistics.asp (Erişim: 16 mart 2009)

[16] Bilişim-İnternet Suçları - İstanbul Basın Savcısı Cevat Özel http://hukukcu.com/modules/smartsection/item.php?itemid=35

[17] Bilişim Suçları Şube Müdürlüğü - http://bilisimsuclari.iem.gov.tr/

[18] Av. Gökhan Gökçe. Siber Güvenlik İstanbul, Şubat 2007 Bilgi Üniversitesi http://bthukuku.bilgi.edu.tr/Documents/gokhan_gokce.ppt

[19] BİDB. SPAM Postalar. http://bidb.pau.edu.tr/SPAMmail.aspx

[20] İnternet Üzerinde Haberleşme, http://ekinoks.cu.edu.tr/İnternet/konu_17.htm

[21] Slettnes, T., Çeviri: Bugüner N.B., “Spam Filtering for Mail Exchangers”, 2004. http://slett.net/spam-filtering-for-mx/
http://www.belgeler.org/howto/spam-filtering.html

[25] The Case For RMX Records.
http://www.mikerubel.org/computers/rmx_records/#notes_spoofing

[26] How to secure your mail system against third-party relay.
http://www.mail-abuse.com/an_sec3rdparty.html

[27] E-mail SPAM. http://en.wikipedia.org/wiki/E-mail_SPAM

[28] Türk Telekom A.Ş. Anti-SPAM & Anti-abuse Grubu.
http://karaliste.ttnet.net.tr/2.html

[31] ODTÜ-BİDB. Bogofilter SPAM filtresi ve SPAMbox uygulaması.
http://www.bidb.odtu.edu.tr/index.php?go=tsg&sub=bogofilter

[32] Emin Can. Posta Sunucuları için SPAM Önleme Araçları.
http://www.belgeler.org/howto/antispam.html

[40] SPAMd. http://en.wikipedia.org/wiki/SPAMd

[41] OpenBSD spamd, http://www.openbsd.org/spamd/

[43] Spam Statistics from TRACE ::Marshall
Statistics for Week ending March 15, 2009.
http://www.marshal.com/TRACE/spam_statistics.asp (Erişim: 16 mart 2009)