POSTA SUNUCULARINDA SPAM ÖNLEME TEKNİKLERİ

Önder Şahinaslan
Bilişim Bölüm Başkanlığı
Maltepe Üniversitesi, İstanbul
onder@maltepe.edu.tr

Emin Borandağ
Bilişim Bölüm Başkanlığı
Maltepe Üniversitesi, İstanbul
eminb@maltepe.edu.tr

Emin Can
Bilişim Bölüm Başkanlığı
Maltepe Üniversitesi, İstanbul
emincan@maltepe.edu.tr

Ender Şahinaslan
Bilgisayar Mühendisliği
Trakya Üniversitesi, Edirne
ender@bankasya.com.tr

ÖZET

Elektronik haberleşmede istenmeyen e-posta oranının arttığı bir dönemde spam saldırılarına karşı güvenli bir ağ trafiğinin olması gerekmektedir.

Ağ güvenliği denildiğinde; yetkisiz erişimlerin engellendiği, bağlı cihazların güncelliğinin sağlandığı, yama kontrollerinin yapıldığı, anti güvenlik yazılımlarının kurulduğu, saldırı iz takibi ve anlık önlemlerin alındığı merkezi bir yapı akla gelir.

Güvenlik açıklarına, kaynak israfına, iş gücü ve zaman kaybına neden olabilen spam saldırılarının engellenmesine yönelik posta sunucu hizmeti veren kurumlara çok daha görev düşmektedir.

Bu çalışmada, kampüs ağlarında bilgi güvenlinin sağlanmasına yönelik spam önleme teknikleri ile ilgili bir araştırma yapılmıştır. Saldırı kaynaklarının yok edilmesi ve dışarıdan gelebilecek spam postaların merkezi sunuculardan ağa girişini engellenmesi amacı ile kampüs güvenlik uygulaması geliştirilmiştir.

Anahtar Kelimeler: SPAM Önleme Teknikleri, Bilgi Güvenliği, Endian, Qmail, Spamdyke, Spamassassin, Clamav

ABSTRACT

It requires to be reliable network traffic against spam mail attacks at the term that unwanted e-mail ratio increases at electronic communication.

Network security means a central structure in which unauthorized access is denied, connected devices are updated, patch installations are checked, security software is installed, attack track and instant precautions are taken.

E-mail service providers have more responsibility about preventing spam attacks that cause security vulnerability, wastage of resources, waste of time and manpower.

This study is about researching by spam measurement techniques that provide information security on campus networks. A campus security application has been developed to eliminate attack resources and block spam e-mails that will be able to come from outside to enter network by central server

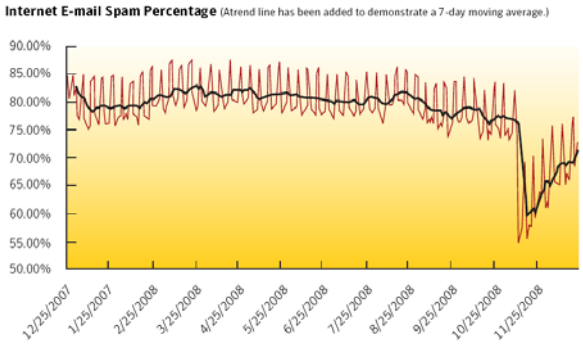
Key Words: SPAM Preventation Techniques, Information Security, Endian, Qmail, Spamdyke, Spamassassin, Clamav

1.GİRİŞ

Bilgisayar ve internet teknolojilerinin yaygın kullanımı ile birlikte, verilere erişim merkezi ve sınırlı olmaktan çıkmış, ağ ortamında uzak mesafelerde dağınık paylaşılabilir hale gelmiştir. Buna e-posta ve web üzerinden gelebilecek tehditlerinde eklenmesi sonucu, bilgi güvenliği ciddi bir nitelik ve boyut değişimine uğramış, önemini daha da artırmıştır.

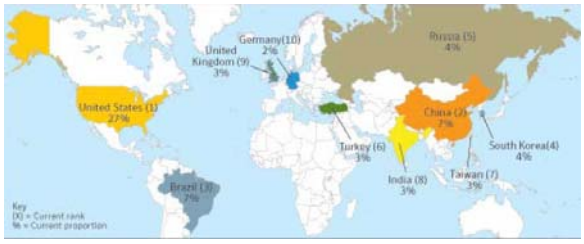
Bireysel internet erişiminin hızlanması ve ucuzlaması ile birlikte ağa bağlı kullanıcı sayısında sürekli artış olup, spam e-posta ile taşınan zararlı yazılımların hareket alanı da genişlemektedir.[1]

Etkileşimli ve sürekli artış gösteren bu iletişimin farkında olan virüs yazılımcıları ve dolandırıcılar, e-posta yolu ile içeriği merak ve ilgi uyandıran eğlence, reklam, duygu sömürüsü, yardım, bankacılık, toplum mühendisliği gibi davetsiz spam nitelikte mailler gönderilmektedirler. Zararlı ve gizli kod taşıyan bu e-postalar kullanıcının adres defteri, internet bankacılığı kimlik bilgi girişi yapılan siteler, mesajlaşma içeriği gibi hassas bilgileri ele geçirmektedirler. Kullanıcılar bu saldırılara karşı mücadele verirken bilgi kaynaklarını, değerli olan zamanlarını ve paralarını kayıp etmektedirler. İstatistiklere göre dünyada e-posta iletişimini sağlayan kaynakların %75'lik kısmı SPAM e-postaların taşınması için kullanılmaktadır. Şekil-1'de de görüldüğü üzere spam oranlarının %50'nin altına düşmediği de görülmektedir.



Şekil-1 Aylara Göre Spam Yoğunlukları

Spam e-postaların coğrafi harita üzerine dağılımına bakıldığında, ABD'nin ilk sırada Türkiye'nin ise 6.sırada olduğu görülmektedir. [2]



Şekil-2 Çoğrafi Spam Dağılımı

Açık kaynak kodlu yazılımlarla spam e-postaların ve zararlı eklentilerin filtrelenmesine yönelik çözüm örneklerini de içeren bu çalışma dört bölüm altında toplanmıştır. 2. Bölümünde SPAM kaynaklı saldırı metotları 3. Bölümünde bilgi güvenliğini tehdit eden spam postalarını önlemek için geliştirilmiş Endian, Spamdyke, Spamassassin ve Clamav yazılımları anlatılmaktadır. 4. Bölümünde spam saldırılarına karşı geliştirilmiş olan örnek kampüs uygulaması üzerinde alınması gereken önlemler incelenmiştir. Son bölümde ise oluşturulan kampüs uygulaması sonucu elde edilen bilgiler verilmektedir.

2. SPAM KAYNAKLI SALDIRI METOTLARI

Elektronik posta**,** günümüzün en yaygın haberleşme uygulamasıdır. Bu kanaldan yapılan spam kaynaklı saldırılar çoğunlukla merak uyandırma, reklam, korku, eğlence, politik, yardım gibi konularla karşımıza çıkmaktadır.

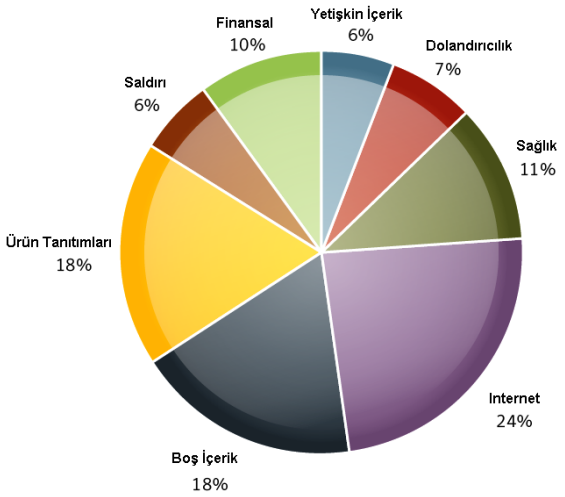
Saldırı amaçlı kişiler ise hedef olarak öncelikle sistemdeki en kolay giriş yolunu yani açıklıkları denerler. Bu yolun önceden saldırı amaçlı çok sık kullanılan bir yol olması gerekmeyebilir. Örneğin sistemde yeni keşfedilmiş bir güvenlik açığı, o anki güncelleme eksikliğinden dolayı hedef olabilir.

Spam postalarla birlikte taşınan virüs vb. yazılımların tespit edilmesi oldukça güçtür. Çok değişik yöntem ve senaryolarla kişinin bilgisayarına gizli bir ajan yazılım olarak yerleşebilmektedir. Kendilerini faydalı bir program olarak göstererek kullanıcının onayını aldığından dolayı çoğu güvenlik önlemleri yetersiz kalabilmektedir. [3]

Uygulamaların sanal ortama taşındığı e-devlet, e-kurum, e-bankacılık gibi işlemlerde kullanılan kullanıcı kimlik doğrulama, hesap ve şifre bilgilerinin elde edilmesine yönelik phishing türü yanlış yönlendirmelerde de kullanılabilmektedir. Gizli DNS ve hosting yanıltma yöntemleri kullanılarak, gelen bir e-postanın gerçek bir bankadan veya kurumdan geldiği izlenimi vermek suretiyle bir takım kişisel bilgileri sahte formlarla istemektedirler. Çok sık yaşanan bu tür mağduriyetlerden dolayı kurumlar web sayfalarından veya SMS ile ilgili, iletinin spam olduğuna dair sürekli uyarıda bulunmaktadırlar.

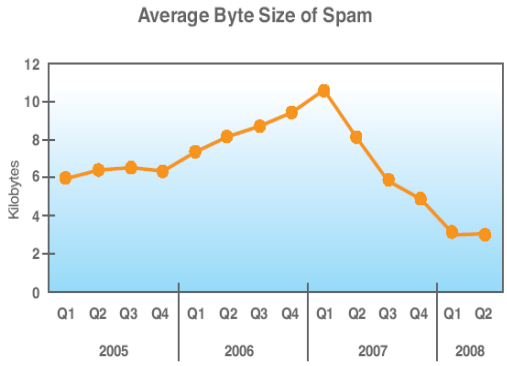
Bilgisayarlarında yeteri seviyede güvenlik önlemlerini almayan kullanıcılar, hem kendileri mağdur olmakta hem de farkında olmadan en yakın arkadaşlarını tehlikeye sokabilmektedirler. Spam yoluyla yerleşen zararlı bir yazılım kişinin Outlook'undan adres defterindeki tüm kullanıcılara kendi adında tuzak olabilecek yanıltıcı postalar gönderebilmektedir. Karşıdaki kişi gelen zararlı eklentiye sahip e-postanın tanıdığı ve güvendiği kişiden geldiği varsayımıyla rahatlıkla onay verebilmektedir. Bu şekilde bilgisayarlara yüklenebilen bir takım yazılımlar klavyeden girilen bilgileri, mouse ve ekran görüntülerini saldırgan hedefe doğrudan göndermektedir. Zehirlenmiş PC olarak tariflenen bu bilgisayarlar üzerinden başkalarına ait binlerce reklam maili gönderilebilir. Uzak masaüstü servisini başlatarak saldırganın doğrudan erişmesini sağlar. İnternet bağlantı türünü değiştirerek milletler arası veya tuzak kontur karşılığı çalışan telefonları çevirerek faturanın yüksek bedelli gelmesini sağlar.

Genellikle e-postalarla taşınan ve istem dışı programların çalışmasına neden olan spamlerin içeriklerine göre internette yayılım dağılımı Şekil -3 de gösterilmiştir.



Şekil-3 Spam E-Postaların İçeriklerine Göre Oransal Dağılımı

Bireyler e-postalarını iletişim adresi olarak ilk sıralarda kullanmakla birlikte kurumlarında ücretisiz bir duyuru aracı olduğu için çok fazla tercih edilmektedir. [4] Böylece her geçen gün önemini daha da artıran e-posta kutusuna gelebilecek yoğun spam postaların ayıklanması sürecinde çok önemli olabilen bir postanında gözden kaçmasına veya silinmesine neden olabilmektedir. [5]



Şekil-4 Boyutlarına Göre Spam Dağılımı

Yukarıdaki şekilde görüldüğü gibi 2005-2006 yılları aralığında taşınan spam e-postaların boyutları resim yoğunluklu olması nedeniyle ortalama 8 KB iken 2007 yılı başından itibaren URL temelli kullanım nedeniyle spam postaarının boyutları ortalama 3-4KB arasındadır. [6]

3. SPAM ÖNLEME TEKNİKLERİ

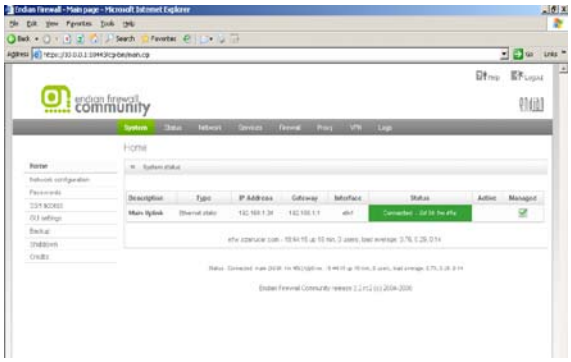
Spam e-postalarla mücadelede sunucu ve istemci tarafında alınması gereken bir takım önlemler vardır. İnternet tabanlı veya Outlook benzeri e-posta okuyucularda önemsiz posta klasörü konfigüre edilerek mutlaka tanımlanmalıdır. Doğrudan tanıma ve öğrenme yeteneği sayesinde daha önce bir kez spam olarak belirtilen bir posta türü artık spam klasörüne gidecektir. Günümüzde Anti-virüs yazılımları sadece virüs temizlemekle kalmayıp diğer anti-spam, anti-trojan, anti-spyware, internet security gibi birçok anti-tarama yeteneği olan tümleşik yazılımlar haline gelmiştir. Kullanılmakta olan güncel anti-virus yazılımının spam tarama özelliği aktif tutulmalıdır. Posta hizmeti veren sunucu sistemlerinde ise domain üzerinden gelen giden tüm e-postalar; içerik, konu, kimden ve ekler olmak üzere birçok kritere göre taratılır. Bu amaçla GFI benzeri pek çok ticari spam önleme yazılımları geliştirilmiştir. Özellikle üniversite ve gönüllü kuruluşların desteği ile ticari sistemlere alternatif olan Spamassassin ve Spamdyke gibi açık kaynak kodlu anti-spam çözümleri üretilmiştir.[7][8]

Spamle mücadelede güncelliğini kısa sürede kaybedebilecek ve sonu gelmeyen ticari yazılım ve donanım ürünleri yerine fazla sistem ihtiyacı gerektirmeyen verimli kaynak kullanımına sahip açık kaynaklı yazılımlarla milyonlarca dolar ulusal kaynak israfından tasarruf edilebilir.

3.1. ENDIAN FIREWALL

Endian Firewall, Linux tabanlı bir yazılım olarak geliştirilmiştir. Oldukça gelişmiş ve yetenekli bir güvenlik duvarı olarak kullanılmaktadır. Endian firewall yapısında başta firewall ve içerik filtreleme olmak üzere pek çok farklı amaca hizmet etmektedir.

Endian firewall sayesinde; Firewall, http Proxy, Smtp Proxy, Antivirüs, Antispam, VPN, gibi pek çok servis kullanılabilir. Kolay ve kullanışlı bir ara yüzü bulunmaktadır. Bu ara yüzün Türkçe dil desteği de mevcuttur. Endian'da dört farklı arayüz tanımlanabilir. Bunlar LAN, WAN, DMZ, WIFI [9][10]



Şekil–5 Endian Firewall Kullanıcı Ara Yüzü

3.2. SPAMDYKE

Qmail posta hizmeti için özel olarak hazırlanmış blacklist kontrolü yapan bir anti spam aracıdır. Kimlik denetiminden geçen kullanıcıların e-posta göndermesine olanak sağlamaktadır. Bu özelliği sayesinde spamdyke Qmail ile yaygın olarak kullanılan Rblsmtpd (blacklist kontrolü) uygulamasının önüne geçmektedir. Bu sayede blacklist kontrolünde daha esnek bir yönetim sağlamaktadır. Aşağıda spamdyke yapılandırmasına ilişkin ana konfigürasyon dosyası verilmiştir.

log-level=2
local-domains-file=/var/qmail/control/rcpthosts
max-recipients=5000
idle-timeout-secs=60
reject-empty-rdns
reject-unresolvable-rdns
reject-ip-in-cc-rdns
greeting-delay-secs=5
check-dnsrbl=zen.spamhaus.org
check-dnsrbl=dul.dnsbl.sorbs.net
check-dnsrbl=bl.spamcop.net
check-dnsrbl=cbl.abuseat.org
check-dnsrbl=list.dsbl.org
check-dnsrbl=ix.dnsbl.manitu.net
reject-missing-sender-mx
rdns-whitelist-file=/home/vpopmail/whitelist_rdns
ip-whitelist-file=/home/vpopmail/whitelist_ip
sender-blacklist-file=/home/vpopmail/blacklist_senders
ip-blacklist-file=/home/vpopmail/blacklist_ip

3.3. SPAMASSASSIN

Spamassassin kural tabanlı bir spam önleme aracıdır. Oluşturulacak kurallara göre bir postanın spam olup olmadığına karar verebilir. Esnek ve gelişmiş programlama arabirimi sayesinde birçok posta sunucuları ve diğer spam önleme aracı ile birlikte bir bütünlük içinde çalışabilir. Bunların başında Razor, Pyzor, Dcc gelir. Ayrıca RBL'leri (kara listeleri) kontrol edebilir ve MX kaydı sorgulaması yapılabilir. [11]

Çalışma mantığı kısaca, iletinin başlık bilgisi, konu kısmı ve iletinin gövde kısmı spam denetiminden geçirir. Denetim sırasında her bir adım için puanlar verilir. Örneğin iletinin konu kısmı boşsa veya büyük harfler içeriyorsa, ileti gövdesi çok fazla HTML etiketi içeriyorsa ya da ileti birden çok kişiye gönderilmişse gibi kriterler göz önünde bulunduruluyor. Bir de bunlara RBL ve MX kontrolü eklenir. Bunların sonucunda yapılan puanlama bizim belirlediğimiz değere göre spam ya da değil şeklinde sonuçlanmaktadır.[12]

3.5. CLAMAV

Clamav açık kaynak kod dünyası için tasarlanmış bir antivirüs yazılımıdır. Kolay kullanımı ve esnek yapısı sebebiyle çok tercih edilmektedir. Otomatik virüs veritabanı güncelleme özelliğine sahiptir. Birçok posta sunucusu ile bütünleşik olarak çalışabilmektedir.[13]

Gelen ve giden tüm e-posta trafiği için taramalar aracılıyla ağ geçidi seviyelerinde antivirüs koruması sağlar. Tam olarak gerçek zamanda mesajların yerel ya da uzaktaki sunuculardan gelmelerini önemsemeksizin tüm SMTP trafiğini ağ geçidi üzerinden doğrudan tarar.[14]

4. KAMPÜS UYGULAMASI

Kampüs içerisinde bilgisayar ve internet kullanımı her geçen gün daha da yaygınlaşmaktadır. Veri iletiminin ve bilgi paylaşımının vazgeçilmez olduğu bir dönemde, değerli olan bilgi kaynaklarımız spam ve diğer zararlı yazılımlara karşı korunmalıdır. Bu kapsamda kampüs uygulaması olarak spam önlemeye yönelik birçok ticari yazılım kullanılmıştır. Bu yazılımların ticari olması ve beklenilen etkiyi sağlamaması nedeniyle açık kaynak kodlu çözümlere geçilmiştir.

Bu doğrultuda öğrenci ve personele ait 12000 civarında posta hesabı Qmail posta sunucusu üzerine taşınmıştır. Çoklu domain desteği, yüksek güvenli yapısı, açık kaynak kodlu oluşu, düşük kaynak

tüketimi ve ücretsiz olması nedeniyle tercih edilmiştir. Bu sunucu üzerinde anti spam aracı olarak Spamdyke ve Spamassassin kullanılmaktadır. Clamav ile tüm e-posta trafiği anti virüs taramasından geçirilmektedir. Aşağıda Spamassassin yapılandırmasına ilişkin ana konfigurasyon dosyasınından bir örnek verilmiştir.

ok_locales all

skip_rbl_checks 1

required_score 4

report_safe 0

*rewrite_header Subject ***SPAM****

use_pyzor 0

use_auto_whitelist 1

use_bayes 1

use_bayes_rules 1

bayes_auto_learn 1

*whitelist_from *@isbank.com.tr*

..

..

*blacklist_from *@garantlbank.com*

..

..

header msg17 Subject =~ /Güvenlik Alarmi!/i

score msg16 100

4.1. QMAIL TOASTER YAPILANDIRMASI

Linux sistemler için geliştirilmiş bir posta gönderi aracıdır. Sendmail programına alternatif olarak geliştirilmiştir. Güvenliği ön planda tutan bir yapısı vardır.

Büyük sistem ihtiyacı yoktur. Yapısı içerisinde farklı domainleri aynı sunucu üzerinde desteklemektedir. Qmail'de posta alımı, yerel sisteme posta gönderme, uzaktaki sisteme posta gönderme, smtp servisini çalıştırma gibi işler için farklı uygulamalar vardır. [15]

Qmail diğer MTA Mail Transfer Agentlara göre daha az bir koda sahiptir. Karmaşık bir yapılandırma dosyası yoktur. Veri güvenliği ön planda tutulmaktadır.

Kampüs uygulamasında qmail toaster versiyonunu kullanılmıştır. Qmail toester versiyonuda uygulamalar Source RPM paketlerinden RPM paketlerine derlenmektedir.[16] Uygulamaları güncellemek, RPM paket yönetimi kullanıldığı için daha kolaydır. Kuyruk yöneticisi olarak Simscan uygulaması kullanılarak domain veya posta bazlı anti virus, anti spam politikaları ayrı ayrı belirlenebilmektedir.[17][18]

4.2 SPAMASSİN YAPILANDIRILMASI

Kullanılan sistem üzerine Qmail toaster yapılanması sonrasında birlikte gelen spamassin toaster paketini kurulur. Temel yapılandırılmada genel spam score seviyesi, black ve white listelerinin oluşturulması otomatik öğrenme ve dil ayarları yapılır. Spam belirlemesi ile ilgili ayarlar bittikten sonra güncelleme ve ek kuralların uygulanması ile ilgili ayarlar yapılır.

4.3. SPAMDYKE YAPILANDIRILMASI

Spamdyke proje sitesinden uygulamanın kaynak kodu indirildikten sonra sistem ihtiyaçlarına göre derlenir. Derleme işlemi bittikten sonra ilk olarak Qmail uygulaması ile çalışılacak şekilde ilgili conf dosyası düzenlenir. Dünya geneline de kabul gören 'black list' ve 'white list'lere ilişkin veritabanı tanımlaması yapılır. Gerek görüldüğünde bu listelere domainler eklenebilir.

4.4. CLAMAV YAPILANDIRILMASI

Clamav proje sitesinden uygulamanın kaynak kodu indirildikten sonra sistem ihtiyaçlarına göre derlenir. Daha sonra posta sistemi ile bütünleşmiş çalışacak şekilde konfigürasyonu yapılır. Konfigürasyon dosyasında anti virüs taraması ve veri tabanı güncellemesiyle ilgili ayarlar yapılır.

4.5. ENDIAN YAPILANDIRILMASI

Endian proje sitesinden uygulamanın ISO dosyasını indirdikten sonra sistem ihtiyaçlarına göre uygun bir donanım üzerine kurulumu yapılır. Gerekli konfigürasyonlar yapıldıktan sonra anti spam yapılandırılması için SMTP Proxy bölümüne geçilir.

Şekil–6 Endian Firewall SMTP Proxy Ara Yüzü

Transparent on GREEN(Green network ten 25. porta gelen tüm istekleri smtp porxy ye yönlendirir.)

Transparent on ORANGE(Dmz ağdaki 25. porta gelen tüm istekleri smtp porxy ye yönlendirir)

Antivirus is enabled(Anti virüs denetimini etkinleştirir.)

Spamcheck is enabled(Anti spam kontrolünü etkinleştirir.)

File extensions are blocked(Posta eklentisinde filtreleme yapar)

Incoming mail enabled(Gelen postayı iç ağdaki hedef posta sunucuya yönlendirir.)

Firewall logs outgoing connections(Firewall üzerinde 25.numaralı port durum trafiğinin kaydını tutar.)

5. SONUÇLAR

Bilgi güvenliğine yönelik tehditlerin şekil ve nitelik değiştirdiği günümüzde, e-posta yoluyla gelen spam saldırıların önlenmesi gerekir. Kurumumuzda yaşanan bu soruna karşı açık kaynak kodlu yazılımlar kullanılarak çözümler üretilmiştir. Açık kaynak kodlu uygulamaların kullanımı ile hızlı, güvenilebilir, düşük maliyet ve özgün kural tanımlama özellikleri nedeniyle tercih edilmiştir.

Bu bileşenler düşük bellek kullanımı sayesinde son derece hızlı tarama yapabilmektedir.

Yapmış olduğumuz üniversite uygulamasında aşağıdaki sonuçlar elde edilmiştir.

- Domain de kayıtlı yaklaşık 12.000 e-posta hesabına gelen günlük ortalama 70.000 spam posta filtrelenmektedir.
- Öncesinde 3 farklı sunucu ile ancak sağlanabilen e-posta hizmeti geliştirilen açık kaynak kodlu yapı sayesinde tek sunucu üzerinde toplanarak kaynak etkinliği sağlanmıştır.
- Ticari yazılımlarda posta taranması esnasında kuyrukta birikmelere neden olurken, kurulan sistemde bu sorun yaşanmamaktadır.
- Kurulan bu sistem ile yaklaşık $15.000 lisans maliyetinden tasarruf edilmiştir.
- Elde edilen posta tarama sonuçlarına göre gelen postalar üzerindeki falsepozitif sayısı azalmıştır.
- Spam ve zararlı eklenti taşıyan postaların, bilgisayarlara ve ağ trafiğine olan olumsuz etkileri azalmıştır.

Sonuç olarak; özellikle kapalı kampüs ağlarında açık kaynak kodlu bu tarz bir altyapının kurulması ile kurumların spam e-postalarla mücadelesin de olumlu sonuçların alınacağı düşünülmektedir.

6. KAYNAKÇA

[1] Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri, Gürol Canbek, Şeref Sağıroğlu, Aralık 2006, Grafiker Yayıncılık, ISBN 975-6355-26-3

[2] The State of Spam A Monthly Report –January 2009 Generated by Symantec Messaging and Web Security , Doug Bowers Executive Editor, p 3

[3]Kampüs Ağ Yönetimi csirt.ulakbim.gov.tr/ dokumanlar/KampusAgYonetimi.pdf

[4] Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme, Canbek, G., Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Eylül 2005

[5] http://www.commtouch.com/site/Resources/statistics.asp Commtouch,

[6] IBM Internet Security Systems X-Force® 2008 Mid-Year Trend Statistics, IBM Global Technology Services, July 2008

[7] http://www.spamdyke.org/

[8] http://spamassassin.apache.org/

[9] www.cehturkiye.com]

[10] www.endian.com

[11]http://www.belgeler.org/howto/antispam.html

[12] http://spamassassin.apache.org/index.html

[13] http://www.clamav.net

[14] http://www.belgeler.org/howto/antispam-clamav.html

[15] http://www.guvenliweb.org.tr/node/2

[16] http://www.qmailtoaster.org/

[17]http://www.belgeler.org/howto/qmail-kurulumu-nasil_qmail-nedir.html

[18] http://cr.yp.to/qmail/guarantee.html