Güvenlik Tehditi Oluşturan Spam Saldırılarına Karşı Önlemler

Önder Şahinaslan[1] Ender Şahinaslan[2] Emin Borandağ[3] Emin Can[4]

[1,3,4] Bilişim Bölüm Başkanlığı Maltepe Üniversitesi, İstanbul
[2] Bilgisayar Mühendisliği Trakya Üniversitesi, Edirne
[1] e-posta: onder@maltepe.edu.tr [2]*e-posta: ender@bankasya.com.tr*
[3] e-posta: eminb@maltepe.edu.tr [4]e-posta: emincan@maltepe.edu.tr

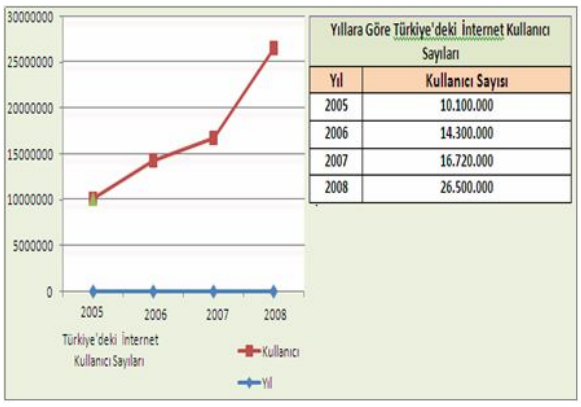
Özetçe

Bilgisayar ve internet teknolojilerinin yaygın kullanımı ile birlikte, elektronik posta sağlayıcıların önemi artmıştır. Elektronik posta hizmeti veren kuruluşlar, sadece postayı iletmekle kalmayıp, kaynak israfına, güvenlik açıklarına, iş gücü ve zaman kaybına neden olan spam saldırılarını engellemeri gerekmektedir. Bu çalışmada, yaklaşık 20.000 kullanıcısı olan üniversite kampus ağında açık kaynak kodlu spam önleme araçları kullanılarak spamden arındırılmış bir posta iletim sisteminin kurulumu anlatılmaktadır.

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

1.Giriş

Günümüzde elektronik haberleşme alanındaki gelişmeler ile birlikte internete erişim yaygınlaşmıştır [1,2]. Dünyada kullanım oranı açısından en fazla performans gösteren ülkeler arasında yer alan Türkiye'dir. Ülkemizde 75,7 milyon kişiden 26,5 milyonu Dünya'da ise yaklaşık 7 milyar kişiden 1,7 Milyar kişinin internete bağlı olduğu gözükmektedir. Bu sayılara bakıldığında %34,5 oranında internet kullanımız olduğunu hazırlanan tabloda gösterilmektedir [3,4].



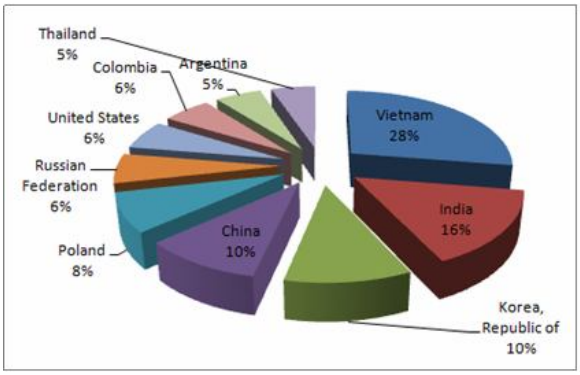
Yıllara Göre Türkiye'deki İnternet Kullanıcı Sayıları

Yıl	Kullanıcı Sayısı
2005	10.100.000
2006	14.300.000
2007	16.720.000
2008	26.500.000

Şekil–1: Türkiye'deki İnternet Kullanıcı Sayıları

İnternet kullanıcısı rakamlarının bu kadar arttığı bir ortamda, internet üzerinden gelen ve sistemlerin güvenliğini etkileyen saldırılarda artmıştır. Zararlı yazılım adı verilen yazılımların hareket alanı da genişlemektedir. Kötü niyetli kişilerin kolay ve hızlı etkileşim kurma imkânı veren bu ortam; amaç dışı, yanlış, yanıltıcı, zararlı ve olumsuz öğeleri içeren teknolojik bir imkân sağlamıştır [5].

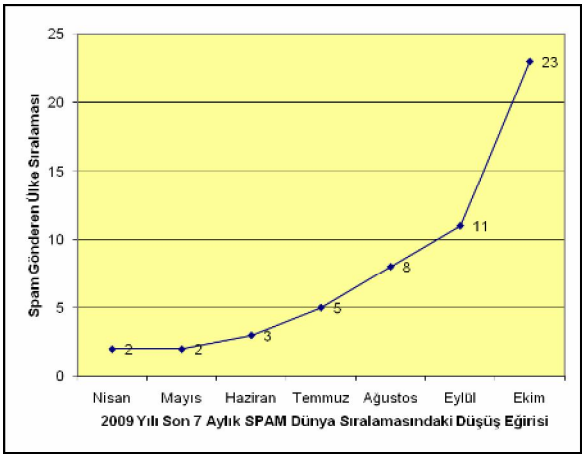
E-posta dünyanın en büyük ve en eski elektronik haberleşme yöntemi olup mesaj okuma, yanıtlama, saklama, gönderme, sıraya koyma, randevu, onay ve bilgilendirme amaçlı kullanılmaktadır. Etkileşimi bir şekilde sürekli kullanım artışı gösteren bu iletişimin farkında olan virüs yazılımcıları ve/veya dolandırıcıları e-posta yolu ile içeriği merak ve ilgi uyandıran; eğlence, reklâm, yardım, duygu sömürüsü, bankacılık ya da toplum mühendisliğini kullanarak kötü niyetlerine davetsiz spam nitelikte e-postalar ileterek kendilerine yeni kullanıcılar aramaktadırlar. Zararlı ve gizli kod taşıyan bu e-postalar ile kullanıcının adres defteri, internet bankacılığı kimlik bilgileri, kullanıcı 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.



Şekil-2: Ülkelere Göre Spam Oranları

Spam e-postaların ülkelere göre dağılım oraları Ekim 2009 itibariyle Şekil-2'de gösterilmektedir. Bu

dağılıma bakıldığında, Vietnam, Hindistan ve Çin gibi ülkelerin ilk sıralarda olduğu görülmektedir.



Şekil-3: Spam gönderen ülkeler sıralamasında Türkiye

Dünyada spam gönderen ülkeler bakımından son yedi ayı gözlemlediğimizde; ülkemizin dünya sıralamasında yeri Şekil-3'de gösterilmektedir. Ülkemiz Nisan-Mayıs aylarında sıralamada en çok spam gönderen ülkeler sıralamasında 2'ci iken sonraki aylara doğru hızla sıralamalarda gerileme yaşanmıştır. Yapılan spam analizlerinde 5–6 ay öncesine kadar ilk 5 içerisindeki yer alan Türkiye'nin TTNET'in STMP portunu kapatması sonrası ciddi bir düşüş yaşanmıştır. Tabi ki bu tarz prot kapatmaları yeni saldırı çeşitliliği yaratarak gibi gözükmektedir. Son olarak yapılan çalışmalarda 587. porttan gelen spamların 587. Numaralı port Kimlik Doğrulaması İstemesine Rahmen arttığı gözlemlenmiştir [6].

Spam e-postaların ve zararlı eklentilerin filtrelenmesine yönelik çözüm örneklerini de içeren bu çalışma 3.Bölümde toplanmıştır. 2.Bölümde bilgi güvenliğini tehdit eden spam postalarını önlemek için geliştirilmiş Endian, Spamdyke, Spamassassin ve Clamav yazılımları anlatılmaktadır Ayrıca bu spam önlemek için geliştirilen yazılımların bir arada nasıl kullanıldığının bilgisi de verilmektedir. Son bölümde ise oluşturulan uygulama sonucu elde edilen sonuçlar verilmektedir.

2. Sunucu Temelli Spam Önleme Yazılımları Ve Kurulumu

Spam aslında Amerikalı'ların meşhur ama geleneksel olmayan konserve et yemeklerinin adıdır. Ancak interneti ilgilendiren boyutu ile ele aldığımızda Internet bağlantısı üzerinde aynı mesajın ya da benzer mesajların yüksek sayıdaki kopyasının, Bu tip mesajları alma isteminde bulunmamış kişilere, zorlayıcı nitelikte gönderilmesi Spam olarak adlandırılır. Spamler çoğunlukla ticari anlamda reklam niteliğinde olup, bu reklamlar sıklıkla güvenilmeyen ürünlerin, çabuk zengin olma kampanyalarının, yarı yasal servislerin duyurulması amacına yöneliktir. Ayrıca virüs içeren Spamler de bulunmaktadır [7]. Spam gönderici açısından çok küçük bir harcama ile gerçekleştirilebilirken mali yük büyük ölçüde mesajın alıcıları veya taşıyıcı, servis sağlayıcı kurumlar tarafından karşılanmak zorunda kalınır.

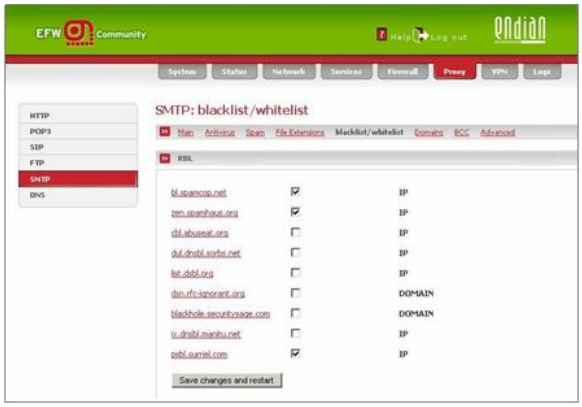
Günümüzde özellikle üniversite ve gönüllü kuruluşların desteği ile ticari sistemlere alternatif olan Spamassassin ve Spamdyke gibi açık kaynak kodlu anti-spam çözümleri üretilmiştir [8].

Kullanılan bu açık kaynaklı sistem çözümleri ile ekonomik anlamda tasarruf sağlanabilmektedir [9].

2.1. Endıan Fırewall Kurulum Ve Konfigürasyonu

Endian Firewall; yazılım da kullanılabilirlik düşünülerek oluşturulmuş kurulumu çok kolay olan gelişime ve değişime hazır olarak geliştirilmiş Linux tabanlı bir yazılımdır. Başta firewall ve içerik filtreleme olmak üzere pek çok farklı amaca hizmet etmek için geliştirilmiştir.Endian firewall ile; Firewall, http Proxy, Smtp Proxy, Antivirüs, Antispam, VPN, gibi pek çok servis kullanılabilir [10,11]. 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 [12].

Endian firewall ile ilgili black listeleri kontrolleri ile ilgili bir ekran görüntüsü Şekil-4'de gösterilmiştir.



Şekil–4: Endian Firewall Kullanıcı Ara Yüzü

Spam önleme için geliştirilen projede gerekli kurulum dosyası belirlenen donanım üzerine kurulduktan sonra gerekli konfigürasyonlar yapılır ve sonraki aşamada spam yapılandırılması için SMTP Proxy bölümüne geçilir. Bu bölümde ki alanlar ve kullanım amacı aşağıda yer aldığı şekilde tanımlanır.

- Transparent on GREEN: Güvenli ağdan 25.nci porta istekleri smtp proxy sunucusuna iletir.
- Transparent on ORANGE: Endian güvenlik duvarının Dmz alanının 25'inci porta gelen tüm istekleri smtp porxy ye yönlendirilir.
- Antivirus is enabled: Anti virüs taramasını gerçekleştirir.
- Spamcheck is enabled: Anti spam filitre uygulamasını aktif hale getirir.
- File extensions are blocked: e-posta üzerinde gelen ekli dosyalarda tarama yapar.
- Incoming mail enabled: Dışarıdan gelen postayı gönderilmesi gereken domaine ait hedef sunucuya iletir.
- Firewall logs outgoing connections: Güvenlik duvarı üzerinden gelen postaya ait durum kayıtlarını tutar.

Tüm bu işlemler ardından Endian Firewall konfigürasyon tanımlaması yapılmış olur.

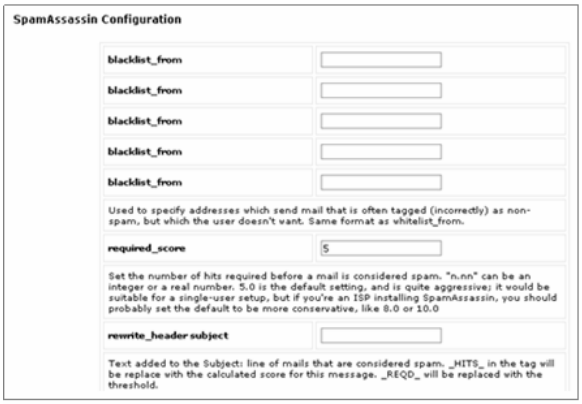
2.2. Spamdyke Kurulum Ve Konfigürasyonu

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.

Uygulamanın kendisi Spamdyke web sitesinden indirildikten sonra sistem ihtiyaçlarına göre kaynak kod derlemesi yapılır. Bu işlemden sonra Qmail posta uygulaması yazılımı ile uyumlu çalışılacak şekilde yeniden yapılandırılır. Yaygın olarak kabul gören 'black list' ve 'white list'nin olduğu veritabanı ilişkilendirmesi yapılır. İlgili servis verilecek domainler Gerek görüldüğünde bu listelere domainler tanımlana bilir [13,14].

2.3. Spamassassın Kurulum Ve Konfigürasyonu

Spamassassin esnek kural tabanlı bir spam önleme yazılımıdır. Gerek duyulan kısıtlamaların önceden tanımlanması yapılır. Tanımlama yapılan konfigürasyon ara yüz örneği Şekil-5'de gösterilmektedir. Tanımlama sonrasında gelen e-postalar bu filtrelemelere göre spam ayrımı yapılmaktadır. Esnek ve gelişmiş programlama arabirimi sayesinde birçok posta sunucuları ve diğer spam önleme aracı ile birlikte bir bütünlük içinde çalışabilir. Black Listeleri kontrol edebilir ve MX kaydı sorgulaması yapılabilir [13,15].



Şekil–5: SpamAssassin Konfigürasyon

Yapısal olarak gelen bir iletinin başlık, konu ve ana metin kısmını içerik denetimi yaparak spam incelemesinden geçirir. Puanlama mantığına göre çalışır. Puanlama işlemi; bir postanın konu kısmının boş olması XML yada HTML kodlarını içermesi, çok fazla kişiye gönderilmesi gibi durumlara bakarak gerçekleştirilir. Bu puanlama durumuna göre e-postanın spam olup olmadığının kararı verilir. Buradaki puan durumu sistemin yöneticisi tarafından belirlenebilmektedir [13,9].

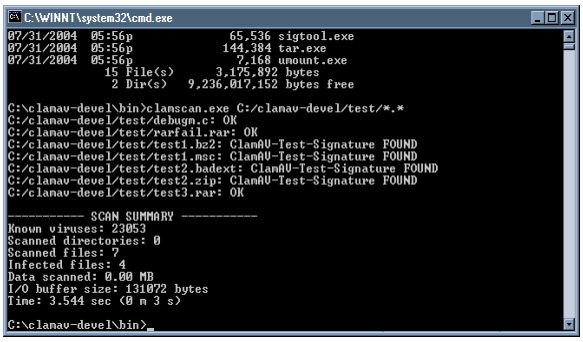
Gerçekleştirilen sistem ile birlikte Qmail toaster paketi ile birlikte gelen spamassassin paketi kurulumu gerçekleştirilir. Güncelleme işleminin ardından alınması gereken ayarlar gerçekleştirilir. black ve white list denilen listeler otomatik olarak oluşturulduktan sonra dil ve automatic learning ayarları gerçekleştirilir.

2.4. Clamav Kurulum Ve Konfigürasyonu

Açık kaynaklı bir anti virüs yazılımı olan Clamav; kullanım kolaylığına sahip olması nedeniyle çok tercih edilen bir programdır. Yapısı içerisinde

otomatik güncelleme özelliğine sahiptir. Pek çok posta sunucusu ile sorunsuz bir biçimde çalışabilmektedir [16].

Bütün network trafiği için taramalar yaparak ağ için anti virüs taramasını ağ geçidi seviyesinde gerçekleştirir. Ağ üzerinden SMTP trafiğini tarama özelliği vardır [13,17].



Şekil -6: Clamav Kurulum ClamAV/SOSDG v▪0▪93▪1-1

Clamav konfigürasyoun için; 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. Örnek Clavav kurulum görüntüsü Şekil-6'da verilmiştir.

2.5. Qmail Toaster Kurulum Ve Konfigürasyonu

Açık kaynak destekli olarak geliştirilmiş bir e-posta sunucu yazılımıdır. Qmail Toaster'ın en önemli özelliği güvenliktir.

Düşük kapasiteli sunuculardada da rahatlıkla çalışabilmektedir. Aynı sunucu üzerinde birden fazla domain desteklenmektedir. Posta alımı, gönderimi ve SMTP servisleri için farklı uygulama desteği bulunmaktadır [18]. Qmail bir diğer özelliği karmaşık bir yapılandırma dosyasına sahip olmamasıdır. Yapılan çalışmalarda iki farklı domain üzerinde Qmail toaster versiyonunu kullanılmıştır. Kurulum aşamasında Qmail toester'a ait source RPM veri paketlerinden derlenmektedir [19].

RPM veri yönetimi sayesinde güncellemesi oldukça kolaydır. Diğer bir avantajı queue management için

Simscan uygulaması kullanılabilmektedir. Bu uygulama sayesinde tüm domain veya kişisel bazlı anti virüs, anti spam içerikli olarak tanımlanabilmektedir [20,21].

Bu yazılımların kurulumu ve konfigürasyonu ile güvenli posta sistemi alt yapısı tamamlanmıştır. Domain ve kullanıcı tanımları sistem üzerinde gerçekleştirilerek kullanıma geçilmiştir.

3. Sonuçlar

E-posta kullanımına olan ihtiyaç her geçen gün artmaktadır. Ancak beraberinde gelebilen spam içerikli postalar ağ trafiğini olumsuz yönde etkilemektedir.

Bu soruna çözüm olarak, üniversite posta sisteminde açık kaynak kodlu yazılımlar konfigürasyonu daha zor olmasına rağmen tercih edilmiştir. Sistemin açık kaynak kodlu olarak tercih edilmesinin nedenleri; yazılımların hızlı, güvenilebilir, düşük maliyetli ve özgün kural tanımlama özellikli olmasıdır.

Sistem kurulumunda anti spam aracı olarak Spamdyke ve Spamassassin kullanılmıştır. Sistem içerisinde, giden ve gelen e-postaların tamamı Clamav anti virüs taramasından geçirilmekte olup bu çalışma sonuçunda elde edilen bilgiler aşağıda belirtilmiştir.

- Her iki domain'e ait yaklaşık 20.000 e-posta tanımlanmış ve bu hesaplara gelen ortalama 100.000 spam posta engellenmiştir.
- Kaynak ihyacı, öncesine göre 2/3 oranında azaltılarak tek bir sunusu üzerinde toplanmış olup kaynak ve maliyet tasarrufu sağlanmıştır.
- Sistem hızı arttığından dolayı daha önce kuyrukta bekletilen e-postalar sorun olmaktan çıkmıştır.
- Yapılan bu çalışma ile yaklaşık $25.000 lisans maliyetinden tasarruf edilmiştir.
- Spam olmayan e-postaların sistem tarafından spam olarak işaretlenmesi sorunu büyük ölçüde giderilmiştir.
- Yapılan çalışma ile güçlü spam ve anti virüs taraması sağlandığından, ağ trafiğinde ve kullanıcı bilgi güvenliğinde olumlu katkısı olmuştur.

Yapılan bu çalışmada; kullanılan açık kaynaklı programların entegrasyonu sayesinde, iki domain'e ait yaklaşık 20.000 e-posta tanımlanmış ve oluşturulan alt yapı ile spam e-postalarla mücadele de olumlu sonuçlar elde edilmiştir. Benzer bir yapının diğer e-posta hizmeti veren sistemleri için de, uygun bir yapı olduğu düşünülmektedir.

4. 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] http://www.internetworldstats.com/ ,Kasım 2009

[3] http://www.finzoom.com.tr/Info/art/News/Turkiye-Avrupa-inte~b28e3b18fcd64106880c27a901a9b409/ ,Ekim 2009

[4] http://www.internetworldstats.com/stats.html ,Kasım 2009

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

[6]http://blog.lifeoverip.net/2009/11/05/ekim-ayi-spam-analizi-turkiye-dunya-spam-siralamasinda-23-sirada/, Kasım 2009

[7] http://www.spam.org.tr/nedir.html, Ocak 2008

[8] http://www.spamdyke.org/, Aralık 2008

[9] http://spamassassin.apache.org, Kasım 2009

[10] www.cehturkiye.com, Kasım 2009

[11] www.endian.com, Mart 2008

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

[13]Posta Sunucularında Spam Önleme Teknikleri, ab.org.tr/ab09/bildiri/81.pdf, Ö. Şahinaslan, E. Borandağ, E.Can, E.Şahinaslan, Şubat 2009

[14] http://www.spamdyke.org/, Kasım 2009

[15] http://www.belgeler.org/howto/antispam.html, Kasım 2009

[16] http://www.clamav.net, Kasım 2008

[17] http://www.belgeler.org/howto/antispam-clamav.html, Kasım 2008

[18] http://www.guvenliweb.org.tr/node/2, Kasım 2008

[19] http://www.qmailtoaster.org/, Mart 2009

[20]http://www.belgeler.org/howto/qmail-kurulumu-nasil_qmail-nedir.html, Kasım 2009

[21] http://cr.yp.to/qmail/guarantee.html, Kasım 2009