

SMTP Sorununa Yeni Bir Yaklaşım: Sistemin Yeniden İnşası

Şükrü Alataş

Gazi Üniversitesi

İktisat Bölümü

salatas@gazi.edu.tr

ÖZET

İlk kez 1982 yılında ufak çapta bir kullanıcı potansiyeli için tasarlanan SMTP sistemi milyarları bulan kullanıcı sayısı ile birlikte sorunlu ve yeni sorunlara açık bir sistem haline gelmiştir. SMTP standardına bağlı olarak ortaya çıkan bu sorunlar başta SPAM, Phishing, Pharming ve Virüsler olarak sıralanabilir. Bu yazıda bu sorunların aşılmasında geçici korunmacı çözümler yerine kalıcı sonuç getiren çözümlerin benimsenmesi, bu çözümlerin sonucunda kısa vadede uyum ve entegrasyon gibi sorunlar ortaya çıksa da uzun vadede ortaya çıkacak sonuçların sorunları kalıcı şekilde anlatılmaktadır.

ABSTRACT

For the first time year of 1982, the system of SMTP was designed for a small group of users but nowadays having more than billion of users at the same time, being a system which is problematic and become a system open for new problems. Spam, Phishing, Pharming and viruses are such general problems becoming depend on the standard of SMTP. At this article based on a idea; instead of applying temporary solutions, the best is adopt solutions radicals, and as a result of these solutions in a short term if there will be some problems like concinnity and integration can be solved by result of long term.

Anahtar Kelimeler: SMTP, SPAM, Phishing, Pharming, Virus

1. GİRİŞ

20. yüzyılın son çeyreğinde ortaya çıkan ve hızla büyüyen internet teknolojisi getirdiği imkânlar ve kolaylıkların yanında birçok sorunu da ortaya çıkarmıştır. Şüphesiz internetin en faydalı olduğu alanlardan biri olan haberleşme alanının en önemli kısmını oluşturan e-posta sisteminin bir açığı olarak ortaya çıkan SPAM ya da diğer söylemi ile istem dışı posta bu kolaylığın önemli bir sorunudur.

2. SPAM ve SPAM'İN DEĞİŞEN YÜZÜ

SPAM kelimesi farklı kaynaklarda farklı olarak tanımlanırken ortak tek bir nokta üzerinde durulur. Bu nokta “istemsiz” kelimesidir. Bir e-postanın SPAM olarak algılanabilmesi için ilk ve en önemli nokta o postanın alıcının istemi dışında gönderilmiş olmasıdır.

SPAM oldukça uzun bir geçmişe dayanan bir kavramdır. Birleşik Devletler Posta Teşkilatının kurulması ile birlikte 20. y.y. başlarında SPAM postalar tüm ülkeye yayılmaya başlamıştır. Teknolojinin ilerlemesi ile birlikte posta yoluyla yapılan SPAM, telefonlar ve faks cihazları üzerinden devam ettirmiştir. Kuşkusuz SPAM en parlak devrini maliyetlerinin en düşük ve etki alanının en büyük duruma ulaştığı yer olan internet ile birlikte yaşamaktadır.

İlk ortaya çıktığı zamanlarda yalnızca reklam ve benzeri amaçlara hizmet eden sorun şu an itibariyle oldukça geniş bir yelpazede ortaya çıkmaktadır. E-posta yoluyla SPAM'in yanında mesaj yoluyla (özellikle ICQ ve AIM üzerinden), forumlar yoluyla, cep telefonu yoluyla ve benzer bir çok yöntemle ortaya çıkmaktadır. Ancak kuşkusuz e-posta yoluyla yapılan SPAM bu pastanın önemli bir dilimini oluşturmaktadır.

Son yıllarda gelişen posta filtreleme yazılımları sayesinde yayılmakta zorlanan SPAM kendisine yeni araçlar ve yüzler bularak ilerlemeye devam etmektedir. Bunlardan en yeni ve önemli bir yöntem olarak Spamdexing gösterilebilir. Bu yöntemin en bilinen alt yöntemi ise “Google Bombing” dir. Google şüphesiz günümüz

internet kullanıcılarının en çok kullandığı arama motorlarından birisidir. 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 yönlendirilmektedir. Bu sayede yönlendirilen sayfanın “rank” i yükselmekte ve böylece sonuç sayfasında yükseltilmektedir. Sonuç olarak belirli bir anahtar kelime sonucunda sadece bu yöntemi kullanarak kendi sırasını yükselten sayfa, kullanıcıların daha çok giriş yaptığı bir sayfa olmaktadır.

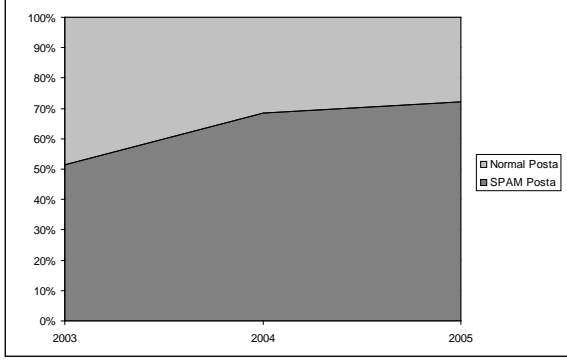
Bu sisteme bağlı ya da bağımsız olarak gelişen yeni bir alt sistemde “Referer SPAM” olarak adlandırılmaktadır. Yine “rank” sistemi dahilinde bulunan “verilen linkler algoritması” sayesinde Google bir sayfaya ne kadar çok başka sayfa tarafından link verilmiş ise o sayfanın “rank“ ini o denli yükseltmektedir. Bu durumdan faydalanarak oluşturulan kod gerçekte var olmayan sayfaları, sayfa taraması yapan googlebot isimli indexleme sistemine gerçek sayfalar gibi göstermekte ve böylece yüksek linklenme oranı ile istenen sayfa yüksek bir “rank” sahibi olmaktadır.

Bu saydığımız iki yöntem dışında SPAM sisteminin yayılması farklı alanlarda ve farklı boyutlarda sürmektedir. Bu çalışma kapsamında inceleyeceğimiz ana sistemsel sorun e-posta sisteminin bulundurduğu açıklar ve bu açıkların çözümünde yeniden oluşturulacak bir e-posta sistemi oluşturulması olacaktır.

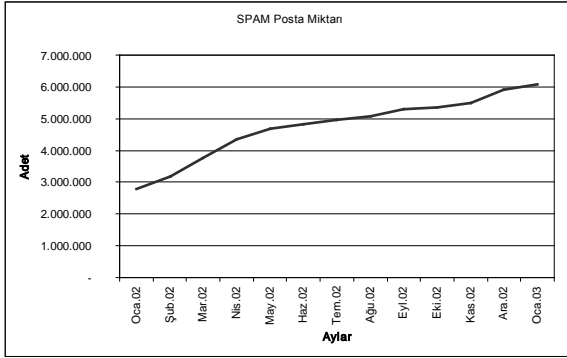
Yazının girişinde belirtildiği üzere günümüzde SPAM ile karşılaşmayan internet kullanıcısı yok gibidir. Her birimizin e-posta adreslerine mutlak ama mutlak günde bir veya birkaç kez SPAM nitelikli postalar gelmektedir. Kullanıcı açısından bakıldığında sorun teşkil etmeyen bir durum gibi gözükse de bu postalar zaman içerisinde katlanarak

artmakta ve e-posta adresinize gelen diğer postaların okunmasını zorlaştırmakta, bazen posta kutunuzu doldurmakta ve kutunun yeni bir posta almasını engellemektedir. Aynı zamanda genellikle reklam amaçlı gönderilen bu postalar müşteri odaklı bir sistemden geçmedikleri için amaç dışı bir reklam da olmaktadır. Ancak gönderimin neredeyse ücretsiz olduğu düşünülürse SPAM postaların belirli bir pazarlama stratejisi kapsamında gönderilmesinin de anlamsız olduğu görülebilir.

SPAM postaların geldiği bu inanılmaz boyutun maddi kısmı da oldukça büyük olmaktadır. 2004 yılında Amerika Birleşik Devletlerinde yapılan araştırma sonucunda SPAM sayesinde gereksiz kullanılan zaman, gereksiz kullanılan bilgisayarların işlem maliyetleri ... vb. eklenerek hesaplanan miktar 10 milyar ABD dolarını bulmaktadır. Bu maliyet yıldan yıla katlanarak artmasına rağmen, her gün yeni çıkan algoritmalarla SPAM postaların filtrelenmesine çalışılmasına rağmen SPAM posta sayısı günden güne artmaktadır. Bir istatistik olarak vermek gerekirse, Grafik 1 incelendiğinde, Amerika Birleşik Devletleri dahilinde internet servis sağlayıcılarından alınan bilgilere dayanılarak oluşturulan istatistiğe göre 2004 yılında %68.6 (her 1,46 e-postadan biri) olan SPAM posta oranı 2005 yılında %72.3 (her 1,38 e-postadan biri) oranına çıkmıştır. Bu sayının 2003 yılı ortalamasının %51.3 olması artışın ne denli hızlı olduğunu göstermek açısından önemli bir rakam olacaktır. Benzer şekilde Grafik 2 incelendiğinde, Ocak 2002 de yaklaşık 2,7 Milyon olan SPAM posta miktarı bir yıl sonra 2003 Ocak ayında 6 milyonun üzerine çıkmıştır. Bu istatistikte genişleyen internet ve e-posta kullanımı sayesinde yüzde oranı olarak artışın nominal değerlerle gösterildiğinde çok daha büyük durumda olduğu göstermektedir.



Grifik 1 - Yıllara Göre SPAM Posta Yüzde Oranı
(Kaynak: Clickz Trends & Statistics)



Grifik 2 – 2002 Yılı Sayısal SPAM Posta Miktarı
(Kaynak: Clickz Trends & Statistics)

SPAM sorunun ne denli hızlı geliştiğini ve ne tür sorunlara yol açtığını gördüğümüze göre bu konuda yapılan yasal düzenlemelere bakabiliriz: Ülkemizde 1997 yılından itibaren konuyla ilgili çalışmalar yapılmakta olup, 2001 yılında Emniyet Müdürlüğü bünyesinde Bilişim Suçları Dairesi kurulmuş bulunmaktadır. 1999 yılından itibaren ise belirli aralıklarla Türk Ceza Kanununda yapılan düzenlemelerle birlikte:

- Bilgisayar Yoluyla Dolandırıcılık TCK 503-507: Dolandırıcılık ve İflas
- Bilgisayar Yoluyla Sahtecilik TCK 316-368: Sahtecilik Suçları
- Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı 5846'nolu Fikir ve Sanat Eserleri Kanunu (FSEK)
- Yasadışı Yayınlar TCK 125-200: Devletin Şahsiyetine karşı cürümler;
- TCK 480-490: Hakaret ve Sövme Cürümleri
- TCK 426-427: Halkın ar ve haya duygularını inciten veya cinsi arzuları tahrik eden ve istismar eder nitelikte genel

ahlaka aykırı: ve diğer anlatım araç ve gereçleri.

- Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim ve Dinleme "Bilişim Alanında Suçlar TCK 525a, b, c ve d". Maddeleridir.

Maddeleri dayanak alınarak işlem yürütülmektedir. Görüldüğü üzere SPAM için spesifik bir yasa bulunmamakta olup postanın içeriğine göre gönderen hakkında hukuki bir yaptırım uygulanabilmektedir. Amerika Birleşik Devletleri 2003 yılında yürürlüğe giren ve halk arasında anti-SPAM kanunu olarak bilinen CAN SPAM yasası dahilinde SPAM ve bağlantılı olan alt sorunlarla savaşta hukuki dayanak yaratmıştır. CAN SPAM kanunu yürürlüğe girdiği 2003 yılından itibaren başta Microsoft olmak üzere birçok firma tarafından yasaya dayanarak SPAM davaları açılmıştır.

3. PHISHING ve PHARMING

Şu ana kadar değindiğimiz SPAM sorunu, genel olarak bakıldığında zaman ve maliyet yaratımı şeklinde ortaya konulabilir. Çünkü SPAM posta almanın size en iyimser pratik zararı posta kutunuzun dolması ve o postayı silerken ya da okurken harcayacağınız zamandır. Ancak aslında yazının ana fikrini oluşturan e-posta açıklarından daha büyük zararlar veren ve çok daha hızla büyüyen bir başka alt sistem olan Phishing – Pharming'e değinmek gereklidir.

Bu iki terim son birkaç yıldır bilişim literatürüne dahil olan kavramlardır. Okunuş itibariyle Fishing (Balık Tutma) ve Farming (Çiftçilik) olarak çevrilebilen bu kelimeler anlam itibariyle de bu kelimeleri karşılamaktadır.

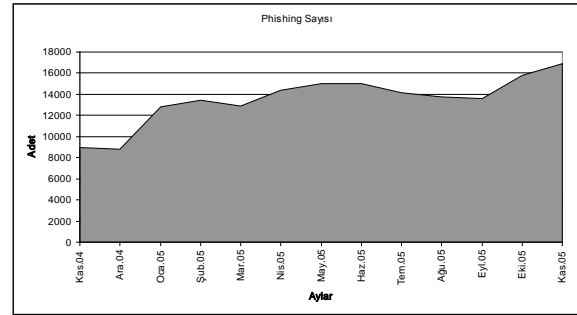
Phishing son yıllarda ortaya çıkmış ve oldukça hızlı bir biçimde büyüyen bir e-posta saldırı sistemidir ve sonuçları SPAM'e göre oldukça ağır olmaktadır. Phishing tekniğinde SPAM de olduğu gibi bir posta listesine bir posta gönderilmektedir. Teknik SPAM'den içerik olarak ayrılır. Phishing'de posta içeriği

alıcıyı yanlış ve ilgi çekici ibarelerle saldırganın sitesine yönlendirme amaçlıdır. Örneğin ülkede yaygın biçimde tanınan bir banka tarafından gönderilmiş gibi gelen bir posta, banka hesabınıza bir hesaptan yüklü miktarda havale yapıldığını ve bu havaleyi onaylamak için belirtilen yere internet bankacılığı kodunuz ve şifrenizi girmeniz gerektiğini tıpkı ilgili bankadan gönderilmiş gibi gelir. Buna isimden anlaşılabilceği üzere “Olta” denir. Eğer alıcı bu olta’yı yutar ve belirtilen yere istenen bilgileri yazarsa Fishing yani balık tutan saldırgan bilgilerini kendi elleri ile vermiş olur. Bundan sonra saldırgan aldığı bilgilerle alıcının hesabından kendi paravan hesaplarına para aktarır.

Pharming yöntemi de benzer bir biçimde olmasına rağmen bazı noktalarda Phishing yönteminden ayrılır. Pharming’de saldırgan “Crimeware” olarak sınıflandırılan programlar yardımcı olur. İlk aşamada gene SPAM yoluyla alıcılara ulaşılır ve yine kandırma yöntemi ile bilgisayarlarına bir program kurdurulur. Bu programlar “tohum” olarak adlandırılabilir. Bu tohumlar bilgisayar açık kaldığı sürece açık kalır ve kullanıcının bütün girdilerini saldırgan iletilir. Bu işlemede “sulama” denir. Kullanıcının banka hesap şifreleri, e-posta şifreleri gibi bilgilerle sulanan tohumlar ürünlerini yine aynı şekilde, kullanıcıların haberleri olmadan yine kullanıcılar kendi elleri ile verirler. Sonuç olarak saldırgan sadece o tohumdan çıkan ürünleri toplamak kalır.

Bu iki yöntemde mağdurlarına oldukça yüklü miktarda zararları olan sistemlerdir. İstatistik olarak vermek gerekirse: 2004 yılında %0.03 olan Phishing oranı 2005 de %0.08 e çıkmıştır. Bu da ortalama olarak her 304 postadan birinin Phishing olduğu 2004 ten 2005’e gelindiğinde her 126 postadan birisinin Phishing olduğunu gösterir. Bu oldukça hızlı bir artışın göstergesidir. Bu istatistiğe bu dönemde artan internet kullanımı sonucunda posta alıcılarının da düşen bilgi seviyesi eklenirse durumun gayet vahim olduğu ortadadır. APWG (Anti

Phishing Work Group) tarafından Kasım 2005 de yayımlanan bildiri de değinildiği üzere Phishing oldukça hızla yayılan ve SPAM’e göre daha ağır sonuçları beraberinde getiren bir sorundur. Aynı raporda değinilen bir başka nokta Phishing yapılırken kullanılan sahte sitelerin ortalama 5,5 gün çevrimiçi kalması ve sonra kendilerini yok etmesidir. Bu sürenin kısıtlı olması mağdurların hukuki süreçte saldırganın izini bulmakta çok güçlük çektikleridir. Çünkü saldırgan ortalama beş buçuk günde kılık değiştirmektedir. Grafik 3’de Kasım 2004 ile Kasım 2005 arasında APWG tarafından saptanan Phishing girişimleri gösterilmiştir.



Grafik 3 – Kasım 2004 ile Kasım 2005 Arası Saptanan Phishing Sayısı

(Kaynak: Anti-Phishing Working Group, “Phishing Activity Trends Report November 2005”)

4. E-POSTA YOLUYLA YAYILAN VİRÜSLER

Yukarıda belirtilen sorunların yanında bir başka sorunda çok uzun yıllardır bilinen ancak kabuk değiştirip e-posta sisteminde faaliyetlerine devam eden virüslerdir. 1999 yılında ortaya çıkan “Melissa” virüsü e-posta sistemi üzerinden yayılmış bilinen ilk virüstdür. 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 mağdurların 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.

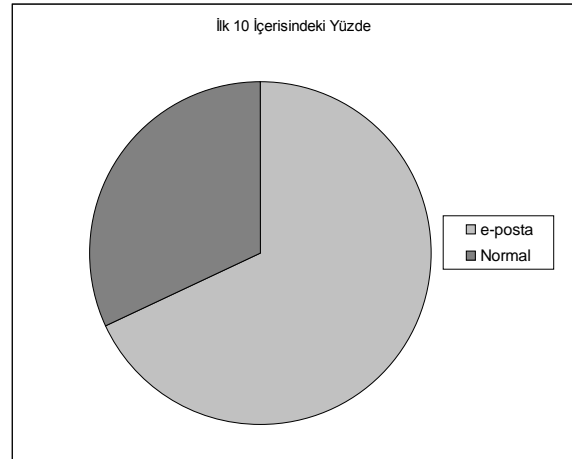
Aralık 2005’de en çok rapor edilen virüslerin oluşturduğu tablo yazının devamında Tablo 1 olarak verilmiştir. Tabloya bakıldığında belirtilen tarihte rapor edilen ilk on virüsü hesaba katılarak bir sınıflandırma yapılması sonucu oluşturulan Tablo 2 den görülebileceği üzere belirtilen tarihlerde en aktif olan 10 virüsün yüzdesel olarak % 67,98’i e-posta yoluyla yayılan virüslerden oluşmaktadır. Bunun yanında normal bilinen yollarla yayılan virüsler sadece %32,02 de kalmıştır. Unutulmaması gereken bir noktada tabloda türü itibariyle “normal” olarak belirtilen virüslerinde yayılma biçimleri arasında posta yoluyla gönderilme bulunmaktadır. Bu açıdan durumun e-postalar yönünde oldukça önemli düzeyde olduğu görülmelidir. Tablo 2 de ortaya konulan veriler Grafik 4 de görsel olarak ortaya konulmuştur.

Sıra	Tür	İsim	Yüzde
1	e-posta	Worm.Win32.Zafi.d	29,17
2	Normal	Worm.Win32.Mytob.c	17,30
3	e-posta	Worm.Win32.LovGate.w	6,07
4	e-posta	Worm.Win32.Sober.y	4,92
5	e-posta	Worm.Win32.Zafi.b	3,73
6	e-posta	Worm.Win32.NetSky.b	3,58
7	e-posta	Worm.Win32.NetSky.q	2,75
8	Normal	Worm.Win32.Mytob.t	2,29
9	Normal	Worm.Win32.Mytob.u	2,28
10	Normal	Worm.Win32.Mytob.q	1,79
		Diğerleri	26,12

Tablo 1 – Aralık 2005 Tarihinde En Çok Rapor Edilen İlk 10 Virüs
(Kaynak: Clickz Trends & Statistics)

Tür	Genel Yüzde	İlk 10 İçerisindeki Yüzde
e-posta	50,22	67,98
Normal	23,66	32,02

Tablo 2 – Aralık 2005 Tarihinde En Çok Rapor Edilen İlk 10 Virüsün Türlerine Göre Yüzde Dağılımı
(Kaynak: Clickz Trends & Statistics)



Grafik 4 – Aralık 2005 Tarihinde En Çok Rapor Edilen İlk 10 Virüsün Kendi İçerisinde Türlerine Göre Dağılımı
(Kaynak: Clickz Trends & Statistics)

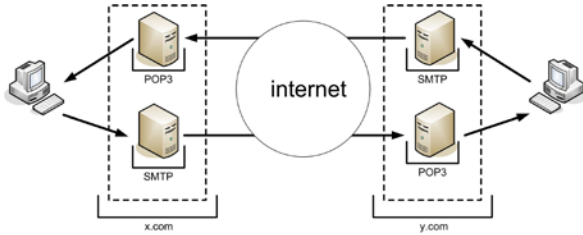
E-posta sistemindeki açıklardan dolayı kaynaklanan sorunlar genel hatları ile özetlenmiş iken, bu sorunların çözülmesi için geliştirilen çözümler oldukça kısıtlı olmaktadır. Aslında genel olarak bakıldığında kesin çözümden öte sadece korunma amaçlı çözümler geliştirilmektedir. İşte bu çalışmanın ana konusu da bu sorunlardan korunmaktan öte sorunu kalıcı şekilde çözen çözümlerin geliştirilmesinde bir adım oluşturabilmektir.

5. ÇÖZÜM

Şimdiye kadar ki ortaya çıkmış genel çözümlere bakıldığında, mevcut çözümler şöyle bir örnekle özetlenebilir. Bir apartmanda oturuyorsunuz ve posta kutunuza gelen reklam postalarından şikayetçisiniz. Bunun için bir çözüm düşünüyorsunuz. Bu esnada bir güvenlik şirketi gelip size apartmanınızın kapısında uygun ücretle bir bekçi koymayı teklif ediyor. Kabul ediyorsunuz. Bu esnada bekçiniz ne kadar maharetli ise kapınızdan giren ve reklam postaları taşıyan insanları o kadar çok engellersiniz. İlk zamanlar gayet başarılı bir çözüm gibi duran bu çözüm zaman geçtikçe reklam getirenlerin işlerinde uzmanlaşması sonucunda yeni dağıtıcıları engelleyebilmek için yeni bekçiler almanız ya da bulunan bekçiyi (güncellenen) sonucu artan mafiyetler olarak kendisini gösterecektir. Sonuçta sonsuza doğru uzayan bir biçimde

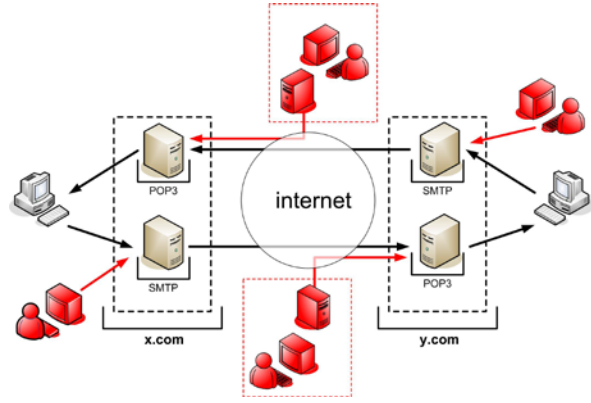
gelişen dağıtıcı, dağıtıcıya bağlı olarak gelişen bekçi şeklinde durum uzayıp gidecek bir sonuca ulaşmayacaktır. En nihayetinde günden güne artan masraflar olarak çözüm size geri dönecektir.

Peki sorun bu durumdayken neden firmalar sorunun çözümüne eğilmeden yüzeysel çözümler sunmaktadırlar? Bu sorunun cevabı gayet açık olarak örnekte bulunmaktadır. Serbest piyasada faaliyet gösteren hangi güvenlik firması kendi maddi kaynağını yok etmek ister. Ya da biraz daha farklı bakış açısı ile eğer dağıtıcılar bir sistemde yok edilebilirse neden güvenlik firmasına ve bekçiye ihtiyaç duyulsun ki! Bu durumda bu sorunun çözümünün güvenlik firmalarından beklenmesi oldukça yanlıştır. Ayrıca detaylı olarak açıklandığı gibi milyar dolarlık bir pastadan pay almak, o pastayı yok etmekten çok daha mantıklıdır. Bu durumda çözüm hükümetlere, sivil toplum kuruluşlarına ve üniversitelere düşmektedir.



Şema 1 – Mevcut SMTP Protokolü Çalışma Sistemi

Sorunun ana kaynağı sistemin kalbindedir. SMTP (Simple Mail Transfer Protocol) posta gönderimi için kullanılan en yaygın protokoldür. Üstte Şema 1’de görülebileceği gibi sistem POP3 protokolü ile birlikte çalışmaktadır. Protokol RFC 821 standardı ile 1982 yılında oluşturulmuş, 1989, 1994, 1995 ve 2001 yıllarında çeşitli düzenlemelerden geçmiştir. Ancak ne kadar güncelleştirilirse güncelleştirilsin 1982 yılında birkaç üniversitenin, araştırma laboratuvarının ve askeri üssün kullanımı için geliştirilen standardın milyarlarca insanın posta ihtiyacına cevap vermesi olanaksızdır. Bu bağlamda soruna çözüm ararken sorunun temeline bakmak şüphesi en doğru yaklaşım olacaktır.



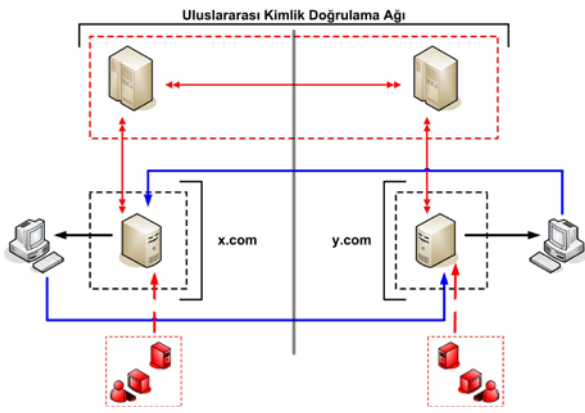
Şema 2 – Mevcut Sisteme Yapılan Müdahaleler

Şema 2 incelendiğinde görülebileceği gibi kırmızı ile belirtilen kötü amaçlı kullanıcılar bazen sunucunun bulunduğu intranet içerisinden bazen de kendi SMTP sunucuları sayesinde internet üzerinden alıcı sunucularını yanıltarak sistemi kendi kötü amaçları doğrultusunda kullanmaktadırlar

Bu bağlamda SMTP protokolü üzerinde yapılacak bir değişiklikten öte kalıcı olarak yeniden yazılacak bir standart ile posta sisteminin yenilenmesi daha efektif bir çözümü sağlayacaktır. Şöyle ki gelişen teknolojiler bünyesinde XML, SSL...vb. veri ve güvenlik teknolojileri ile birlikte bir uzman kurul tarafından belirlenecek yeni standartlarda kullanıcılardan kimlik doğrulanması istenecektir. Düşük bir meblağ ile sadece yetkili kurum tarafından alınabilecek bu kimlikler ya da sertifikalar gönderim esnasında postaya program tarafından eklenecek ve sunucu tarafından bir anlamda imzalanmış gibi işlem görecektir. Bu sayede hem internet kullanıcılarının kullanmadıkları onlarca posta adresi yerine sadece bir ya da iki posta adresleri olacak ancak bu adreslere gelecek herhangi bir kötü amaçlı posta bir sistemle anında sertifika sağlayıcıya bildirilecek ve sertifika sahibine yasal yaptırımlar uygulanabilecektir.

Şema 3 de gösterilmeye çalışılan yazılan teorik önerilerin daha pratikleştirilmiş halidir. Görülebileceği üzere POP3 ile bağlaşıklık bir gönderim protokolü yerine daha kapsamlı tek bir sunucu önerilmektedir. Aynı zamanda gönderimler sunucu vasıtası ile

değil direkt olarak kullanıcılar tarafından yapılmaktadır. Bir e-posta göndermek isteyen kullanıcı alıcı tarafın sunucusuna eriştikten sonra kendi kimliğini üstte belirtilen kimlik doğrulama ağına doğrulattıktan sonra sunucuya postasını bırakır. Eğer geçersiz kimliğe sahip bir kullanıcı sisteme erişmeye çalışırsa sistem doğrulama ağı kimliği kabul etmez ve alıcı sunucu e-postayı reddeder. Doğru kimliğe sahip bir kullanıcı kimliğini kötü bir amaçla kullanırsa alıcı tarafından yapılan başvuru sonucu kimliği iptal edilir ve yasal yaptırım uygulanır.



Şema 3 – Önerilen Protokolün Çalışma Sistemi

Bahsedilen örnekle şu şekilde ifade edilebilir. Yine bir apartmanda oturuyoruz, yine istem dışı gelen reklamlar sorun teşkil ediyor. Bu sefer kapıya bir bekçi koymak yerine kapıya bir turnike yerleştiriyoruz. Kapıdan girerken tekil olarak verilmiş kartlardan kullanılan bir turnike. Bu turnikeden geçen birisi bizim posta kutumuza bir reklam postası bırakmış ise postanın üzerinden kimliğini okuyor ve turnikemizden bir daha geçmesini engelliyoruz. Ayrıca diğer apartmanlarla aramızdaki ağ sayesinde bu kişinin bir başka apartmana da girmesini tamamen yasaklıyoruz. Bu yöntem önceki yönteme göre çok daha efektif bir yöntemdir.

Bu sistemde karşılaşılabilecek sorunlar neler olabilir:

- Sistemin belirli bir ücreti beraberinde getirmesi ile birlikte bedava olan günümüz sistemine göre çekiciliğinin az olması

- En yüksek ihtimalli sorun olarak ise pastanın ortadan yok olması gibi bir durum söz konusu olacağı için güvenlik şirketlerinin takınacağı tutumlardır.

Sistemin daha ufak çapta bir örneği olarak ülkemizde Tübitak ya da Ulakbim çerçevesinde oluşturulacak bir kurul tarafından düzenlenecek standart sayesinde pilot olarak üniversite öğretim üyelerine verilecek kimlikler sayesinde sistem ülkemiz üniversiteleri arasında kullanılabilir ve hataların ayıklanması ile birlikte ülke çapında kullanıma açılabilir. E-İmza'nın kimlik dağıtım esnasında kullanılabilir ve uluslar arası bir standart haline getirilebilir.

6. SONUÇ

Sonuç olarak SMTP sistemi sorunlu ve yeni sorunlara açık bir sistemdir. Bu sorunları aşmada geçici korumacı çözümler yerine kalıcı çözüm getiren çözümlerin benimsenmesi kısa vadede uyum ve entegrasyon gibi sorunlar ortaya çıkarsa da uzun vadede ortaya koyacağı sonuçlar açısından kesinlikle çok sağlam olacaktır.

KAYNAKLAR

- [1] BURNS, Enid, "The Deadly Duo: Spam and Viruses, December 2005", Clickz Trends & Statistics, <http://www.clickz.com/stats/sectors/email/article.php/3577601> (13.01.2006),
- [2] BERNSTEIN, D. J., "SMTP: Simple Mail Transfer Protocol", <http://cr.yip.to/smtp.html>
- [3] Wikipedia, "Spam (electronic)", http://en.wikipedia.org/wiki/Spam_%28electronic%29 (01.10. 2001 – 20.01.2006),
- [4] WEGERT, Tessa, "Spam: Not Just for E-Mail Anymore", Clickz Trends & Statistics, http://www.clickz.com/experts/media/media_buy/article.php/3576741 (12.01.2006),
- [5] STRAUSSER, Kirk, "History of SMTP", http://www.circleid.com/posts/history_of_smtp/ (24.02.2005),

- [6] GREENSPAN, Robyn, "The Deadly Duo: Spam and Viruses, January 2004", Clickz Trends & Statistics,
<http://www.clickz.com/stats/sectors/email/article.php/3308091> (04.02.2004),
- [7] Anti-Phishing Working Group, "Phishing Activity Trends Report November 2005",
<http://www.antiphishing.org/> (08.11.2005),
- [8] Federal Trade Commission, "Cross-border Law Enforcement Team Targets Spammers",
<http://www.ftc.gov/opa/2005/12/buttonpushers.htm> (20.12.2005),
- [9] MARA, Janis, "The Marketing of Can Spam", Clickz Trends & Statistics,
<http://www.clickz.com/news/article.php/3297891> (12.01.2004),
- [10] GREENSPAN, Robyn, "Unwanted Valentines Flood Inboxes", Clickz Trends & Statistics,
<http://www.clickz.com/stats/sectors/email/article.php/1591431> (21.02.2003),
- [11] Wikipedia, "Computer Viruses",
http://en.wikipedia.org/wiki/Computer_viruses (09.12.2001 - 20.01.2006),
- [12] Wikipedia, "Melissa (Computer Worm)",
http://en.wikipedia.org/wiki/Melissa_%28computer_worm%29 (28.01.2003 – 18.01.2006),
- [13] ÖZEL, Cevat, "Bilişim - İnternet Suçları",
http://www.hukukcu.com/bilimsel/kitaplar/bilisim_internet_suclari.htm (24.12.2002)
- [14] İstanbul Emniyet Müdürlüğü Bilişim Suçları Büro Amirliği, "Bilişim Suçları",
<http://www.iem.gov.tr/iem/?m=4&s=51> (2004),
- [15] CASSINGHAM, Randy, "Getting Rid of Spam",
<http://www.spamprimer.com/> (Mart 2005),
- [16] Webopedia, "What is CAN-SPAM?",
http://www.webopedia.com/TERM/C/CAN_SPAM.html (14.12.2004),
- [17] Web Sense Security Labs, "Phishing and Crimeware Map",
<http://www.websensesecuritylabs.com/charts/mapdetails.php>
- [18] Wikipedia, "Google Bombing",
http://en.wikipedia.org/wiki/Google_Bombing (02.08.2003 - 19.01.2006)