SMTP Protokolü ve Spam Mail Problemi

M. Erkan Yüksel[1], Şafak Durukan Odabaşı[1]

[1] İstanbul Üniversitesi, Bilgisayar Mühendisliği Bölümü, İstanbul

eyuksel@istanbul.edu.tr, sdurukan@istanbul.edu.tr

Özet: Spam olarak bilinen, büyük boyutlu, istenmeyen mesajların gelişigüzel bir şekilde gönderilmesi amacıyla elektronik mesaj servislerinin kötüye kullanılması, güvenli postaları da içeren elektronik posta servislerini şüpheli hale getirmekte ve spamlere karşı yürütülen savaşta güçlü bir hedef olmasına neden olmaktadır. Elektronik posta sisteminin spam gönderen kişiler tarafından kötüye kullanılmasının nedeni, bu sistemlerin izlenebilirlikten ve iletişim halindeki varlıkların doğrulamasının yapılmasından yoksun olmasından kaynaklanmaktadır. Bu çalışmada spam göndericilerin davranışlarını analiz etmek amacıyla bir mail değişim sunucusu simüle edilerek, antispam/antivirüs filtresinden mesaj logları ve DNS blok listesinden blocklist logları analiz edilmiştir.

Anahtar Sözcükler: Spam, mail, SMTP,DNSBL.

SMTP Protocol and Spam Email Problem

Abstract: The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages, known as spamming, has made the email systems including the legitimate emails become suspect and has led to substantial investment in thefight against spam. The spammers have abused the email system because of its lack of accountability and verifcation of the communicating entities. In this work, a mail exchange server has is simulated to analyze spammers' behaviours, antispam/antivirus filter message logs and DNS blocking logs.

Keywords: Spam, mail, SMTP, DNSBL.

1. Giriş

İnternetin büyümesi, geniş bir alana yayılması ve popülerliği, elektronik mail iletişimi gibi daha elverişli servislere öncülük etmektedir. Elektronik mail, en çok tercih edilen elektronik iletişim metotlarından biridir ve birçok şirket, kişi ve satıcı, elektronik mailin uygulanabilirliğini kolaylaştırmak için mail altyapısına yoğun bir şekilde yatırım yapmıştır.

Bütün bunlara rağmen, gizli işlerinde kullanmak için ücretsiz mail altyapılarını tercih eden kimseler de bulunmaktadır. Bunlar, elektronik mail iletişim altyapısında inşa edilmiş güvenlik ve güvenilir varlıkların yokluğundan yararlanmışlardır.

2. Mevcut Mail Teknolojisi

İnternet üzerinden email alımı ve iletimi mevcut bir açık standart protokolü kullanılarak gerçekleştirilir: Basit Mail İletim Protokolü (Simple Mail Transport Protocol – SMTP). Mail dağıtımı, bağlantı hostu ile alıcı host arasında bir SMTP işlemini içerir.

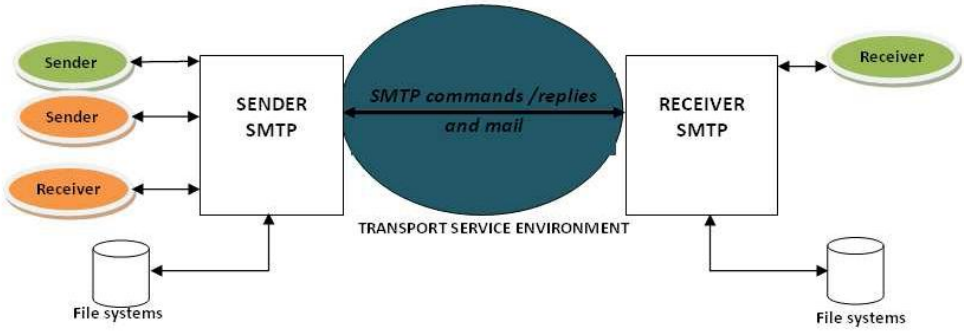
Daha spesifik olarak, bir email için, gönderici SMTP sistemi maili internet içine gönderir; alıcı ya da dağıtımcı sistem maili bir taşıma servis ortamından kabul eder ve mail kullanıcı temsilcisine aktarır ya da mail kullanıcı temsilcisinin erişeceği mesaj deposunda saklar.

SMTP şu iletişim modeline sahiptir: bir kullanıcı mail isteğinin sonucu olarak, gönderici SMTP, alıcı SMTP'ye doğru iki yönlü bir iletim kanalı oluşturur. Alıcı SMTP son hedef olabileceği gibi ara geçişlerden biri de olabilir. Gönderici SMTP, alıcı SMTP'nin yorumlayabileceği ve cevap verebileceği SMTP komutları üretir.

İletim kanalı kurulduğunda, gönderici SMTP, mailin göndericisini belirten MAIL komutunu yollar. Eğer alıcı SMTP maili almayı kabul ederse, bir OK cevabı yollar. Bunu gönderici SMTP'nin mailin alıcısını içeren RCPT komutunu göndermesi izler.

Eğer alıcı SMTP, bu alıcı için maili almayı kabul ederse, OK ile cevap verir; kabul etmezse, tüm mail iletimi için değil sadece bu alıcı için red cevabını döndürür; böylelikle gönderici ve alıcı SMTP'ler aynı kanaldan başka alıcılar için görüşebilirler. Alıcıların başarılı bir şekilde görüşmesi sağlandığında, gönderici SMTP özel bir karakterle sonlanan mail verisi üretir. Mail verisinin başarıyla alınmasından sonra alıcı SMTP OK cevabı döndürür. Bu noktada gönderici SMTP iletim kanalının kapatılması işlemini başlatır.

Eğer gönderici ve alıcı hostlar aynı iletim servisine bağlıysa ya da Şekil 1'deki gibi aynı iletim servisinde değillerse ama bir ya da daha fazla SMTP sunucusu üzerinden bağlanıyorlarsa, SMTP protokolü mailin gönderici hosttan alıcı hosta direk transferine izin verir.



Şekil 1. SMTP mail iletim şeması.

Bir SMTP örneği Şekil 2'de gösterilmiştir. Gönderici bir bağlantı kurar ve alıcı bağlantıyı kabul ya da reddeden bir mesaj koduyla cevap verir.

Herhangi bir SMTP sistemi, başka bir SMTP sisteminden mail alabilir ya da gönderebilir. Yukarıdaki SMTP oturum örneğinde alıcı SMTP sadece iki kimliğe ihtiyaç duyar: göndericinin kimliği ve FROM adres kimliği. Bu kimlikler sahte de olabilir, çünkü SMTP protokolünün kimlik doğrulamak için dahili bir mekanizması yoktur.

Mevcut SMTP mail sisteminin kötüye kullanıma açık olduğu rahat bir şekilde görülebilinir. Öyle ki, herhangi bir gönderici, sahte bir kimlikle, istediği sayıda maili, istediği herhangi bir içerikle, herhangi bir alıcıya rahatlıkla gönderebilir. Elektronik mesajlaşma sistemlerinin rasgele, istenilmeyen emailler yollamak için kötüye kullanımına spam denir. Birinin mail kutusunda bir gün içinde göndericisi bilinmeyen postaların görülmesi çok yaygındır. Bu spamler internette sosyal mühendislik yoluyla siber dolandırıcılık

olarak tanımlanmıştır. Bir çoğu, açıldığı zaman kullanıcının makinesini riske atabilecek bir URL içeren, bilinmeyen bir kaynaktan gelmiş, bir emaille başlar.

Spamin ekonomik olarak yapılması kolaydır, çünkü spam göndericileri sadece kendi mailleşme listelerini yönetirler ki bunun maliyeti oldukça düşüktür.

Ayrıca mailleşmelerinden dolayı sorumlu tutulmaları da zordur. Spam ticaretindeki minimal yatırımdan kaynaklı, spam üreticileri çok sayıdadır ve bu da spam mail trafiğinin yoğunluğunu arttırmaktadır.

Bunun maliyetini yüklenen ise, halk ile bu trafikle başa çıkmak için ağlarının kapasitesini arttırmaya çalışan İnternet Servis Sağlayıcıları olmaktadır.

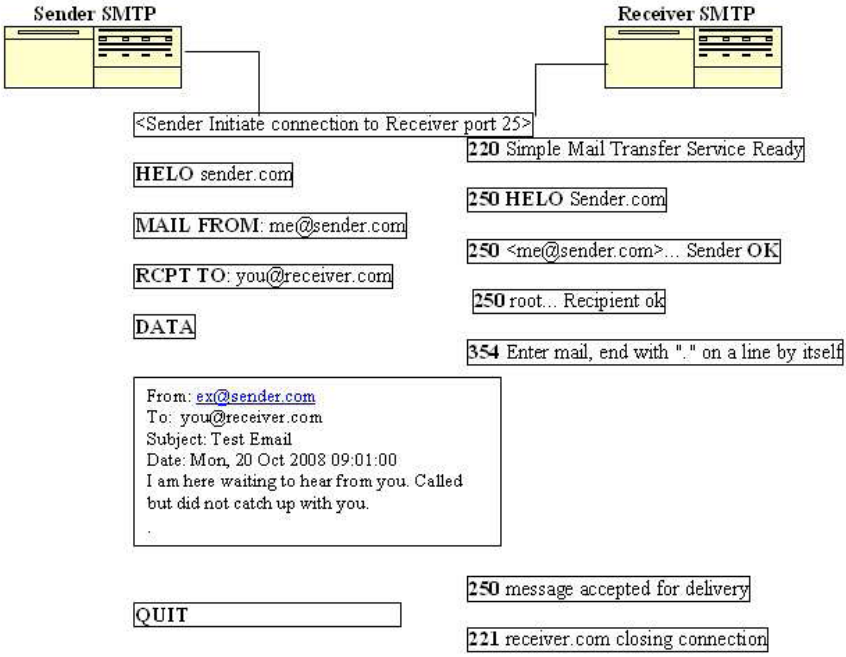
Bütün bunlar, her emailin şüpheli hale gelmesine ve spamlere karşı yürütülen savaşta önemli yatırımlara, spam filtreleyici yazılımlar üreten satıcılara, Alan Adı Sistemi kara listeleri (DNSBL) ve beyaz listeler kullanılarak spam bloklanmasına ve spam üreticilerin aktivitelerini analiz eden araştırmacıların ortaya çıkmasına neden olmuştur.

Spam maillerden kaçınabilmek için, mail sistemlerinin kullanıcıları ve şirket yöneticileri tarafından çok çeşitli araçlar ve anti-spam teknikleri kullanılmaktadır. Bu tekniklerden bazıları, mail sistem kullanıcılarının ve yöneticilerinin spame karşı savaşını kolaylaştırmak için ürünler, servisler ve bunlarla ilişkili yazılımlar içine gömülü haldedir.

Spamlere karşı tamamen başarılı bir çözüm ya da teknik bulunmamaktadır.

Spam probleminin çevresinde yapılan mevcut çalışma, mail sunucu ve/veya mail istemci tarafındaki spam filtresi uygulamasıdır. Spam filtreleme üç metoda dayanır: beyaz listeler, siyah listeler ve email içeriği ya da bunların kombinasyonudur. Mail sunucusunda uygulanan siyah liste filtrelemesi, DNS kara listesinde yayınlanan IP alanına dayanırken, beyaz liste filtrelemesi daha çok istemci tarafında, bir kullanıcının email almasına izin verilen kullanıcı hesaplarına dayanır. Hatta spam filtrele, spam probleminin çözümünde minimal etki yapmaktadır. Spam göndericiler, bu eylemlerini devam ettirebilmek için daima değişim geçirerek yeni teknikler bulmaktadırlar.

Spam probleminin çözümü için mevcut email sistemine revizyon yapılmalı ve izin tabanlı bir sisteme dönüştürülmelidir. Sıkı bir şekilde kurulan açık SMTP email sisteminde tamamen yeni bir protokol uygulanması hem zordur hem de bunun sisteme eklenmesi tüm internet boyunca yeni bir sistemin dağıtılmasının yaratacağı karmaşıklığa neden olur.



Şekil 2. SMTP oturum kurulumu.

3. SMTP ve Spam ile İlgili Yapılan Çalışmalar

Spam aktiviteleri ve altyapıları üzerinde son zamanlarda bir çok araştırma yapılmaktadır. Pathak, Hu ve Mao'nun ortaya koyduğu, spam yollayıcıların global davranışlarının analizi üzerine yaptıkları çalışmada spam yollayıcılar, Yüksek Yoğunluklu Spam Yollayıcılar (High Volume Spammers – HVS) ve Düşük Yoğunluklu Spam Yollayıcılar (Low Volume Spammers – LVS) olarak sınıflandırılmıştır [1]. Kanich, Kreibich ve Levchenko'nun yapmış olduğu çalışmada ise botnet altyapısı kullanılarak ekonomi ve kâr bakımından mail spam piyasası incelenmiş ve spam pazarında düşük yatırımın büyük gelir getirdiği gözlenmiştir [2].

Spam yollayıcı ağı altyapısının varlığı, ağın nasıl genişlediğini ve servis içinde bulunduğunu göstermektedir [3][4]. Yapılan çalışmalar sırasında, spam problemi araştırılmış ve spame karşı mücadelede kullanılacak olan email spam imzasının üretilmesi için botnet tabanlı spam hareketlerinin dağıtılmış karakteristiklerinden yararlanılmıştır [5]. Mesaj boyutları, gönderici, alıcı ve mesaj teslim süresi bilgilerini içeren bir mail sunucusu incelenirse, mail sistemleri için kriter olarak kullanılabilecek mail kalıpları üretilebilinir [6].

SMTP Yol Analizi'ni inceleyen çalışmalarda, mail domainleri ve ilgili IP adreslerinin reddedilme oranını tahmin edecek bir öğrenme algoritması geliştirilmiştir [7]. Bu analizlerin temeli, bilinen güvenli mailler ve bilinen spamlerin iletimi için kullanılan yollar bulunmaktadır. Bunların dışında, veri madenciliği kullanılarak mesaj iletim uygulamasının nasıl gerçeklendiğini inceleyen çalışmalar da, davranış tabanlı mail analizi için yapılan spam tespitinin bir parçası olabilir [8].

Tüm bu çalışmalar, izin tabanlı bir servis sunmayan SMTP protokolünün dizaynının

başında tahmin edilememiş spam probleminin ne kadar önemli olduğunu göstermektedir.

3. Uygulama

Bu çalışmada bir iç mail sunucusu ve dışsal mail sunucuları simüle edilerek, mesaj logları incelenmiştir. Bu iç mail sunucusunun email başlıklarının sinyallerinin mail değişim depolarından elde edilen veriler analiz edilmiştir. Bu veri, DNSBL ve anti-spam uygulaması kullanılarak filtrelenmiştir. İki adet veri seti ile çalışılmıştır. İlki DNSBL bloklama listesidir. Bu veri, "<ZamanDamgası>, <IP Adresleri>, <OK-REJECT>" bilgilerini içermektedir. OK, IP adresinin DNS kara listesinden (DNSBL) geçtiği anlamına gelmektedir. REJECT ise mailin DNSBL kontrolünden geçemediğini göstermektedir.

İkinci veri seti, Anti-Spam Filtre veri logu ise, "<ZamanDamgası>, <IP Adresleri>, <HostIsimleri>, <Olasılık–VİRÜS>" bilgilerini kapsamaktadır. DNSBL kontrolünden geçen her mail, mail sunucusunda filtreleme kurallarına uygun olarak 0 ile 1 arasında olasılıklarla işaretlenmek üzere Anti-Spam filtre aracına gönderilir. Eğer mail virüs içeriyorsa VIRUS olarak işaretlenir.

Spam mailleri, güvenli maillerden ayırmak için, güvenli mail mesajları 0 ve 0.5 arasında olasılıkla işaretlenmiştir. 0.5'den büyük değerlere sahip mailler ise spam olarak belirlenmiştir.

Mesaj loglarının incelenmesi sonucunda elde edilen veriler tablolar halinde hem iç hem de dış mesaj logları için çizelgelenmiştir.

Şekil 3 ve 4'de iç mesaj loglarının sonuçları görünmektedir. Şekillerde bir aylık periyot için, saatlik güvenli ve spam mail sayıları görülmektedir.

Saatler arasında mail aktivitesinin yüksek olduğu zamanlarda, spam hareketliliği de artmaktadır. Başka bir ilginç sonuç ise, Şekil 5'de gösterilen, aynı sunucudan gelen güvenli ve spam mailler arasında güvenilir maillerin sayısının çok olduğunun görülmesidir. Simüle edilen iç mail sunucusundan 1 saat içinde alınan güvenilir maillerin ortalama sayısı 1440 iken, ortalama spam mail sayısı 222 olarak gözlenmiştir.

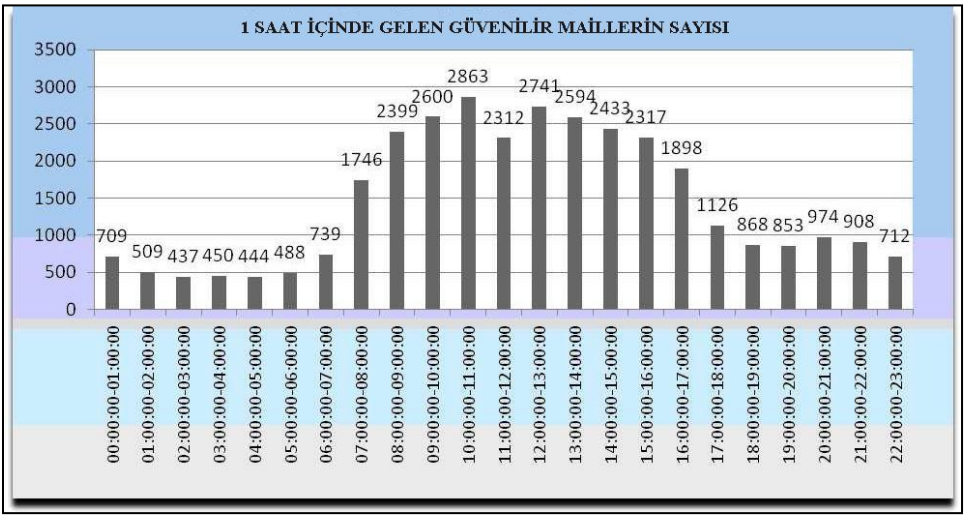
Şekil 6,7 ve 8'de ise yine bir aylık periyot için saatlik dışsal mail log analizi gösterilmektedir.

4. Sonuç

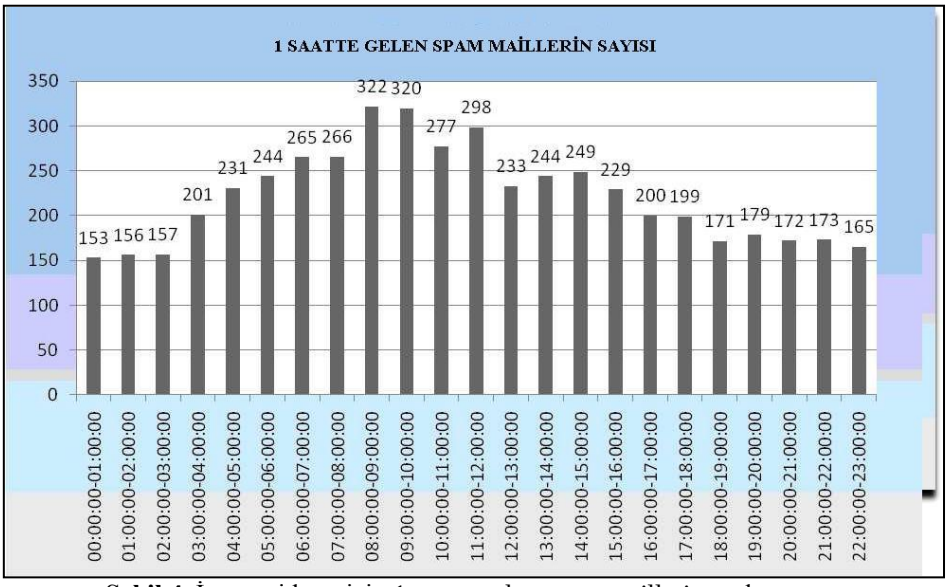
Elde edilen sonuçlar, spam aktiviteleri hakkında aydınlatıcı olmaktadır. Hem iç hem de dış sunuculardan gelen mailere göre, alınan mail sayısıyla beraber spam mail sayısı da artmaktadır ve bu değer gece yarısından önce tepe noktasına ulaşmaktadır.

Spam mailler hem iç hem de dış sunuculardan gelmektedir. Bu esnada birçok mail DNSBL'in kontrolünden tespit edilmeden geçmeyi başarmıştır. Bu durum dinamik IP adreslerinin kullanımı veya spam üreticilerin bot makineler üzerinde çalışmaları ve buna bağlı olarak DNSBL filtrelemeden kaçabilmeleriyle açıklanabilir.

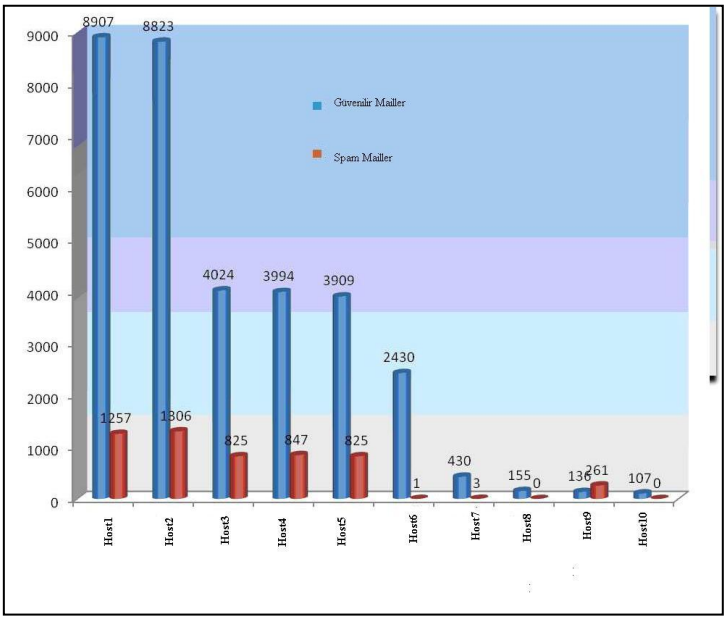
Verinin analizi sonucu, spam mailler filtrelendiğinde, spam yollayıcıların, spam mail göndermeye devam ettikleri; yani filtrelemenin spam yollayıcıları durduramadığı ve bazı spamlerin doğal olarak yayıldıkları gözlenmiştir.



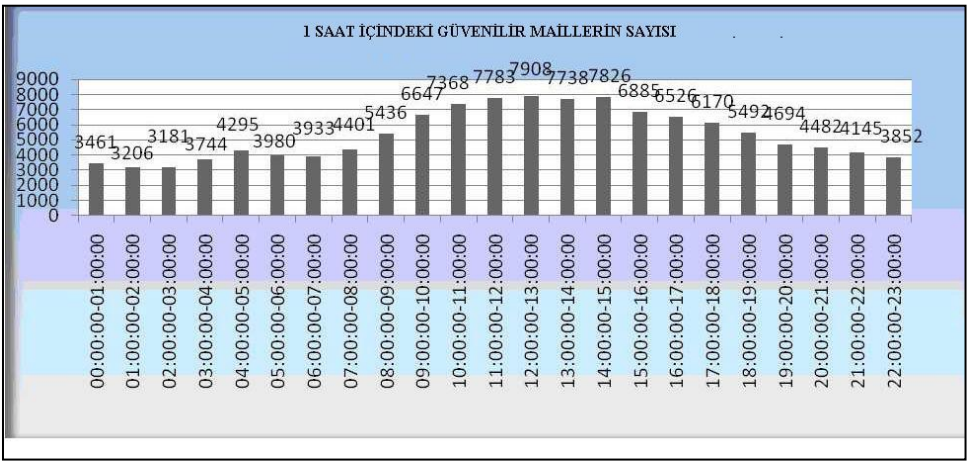
Şekil 3. İç mesaj logu için 1 saatte gelen güvenilir maillerin toplam sayısı .



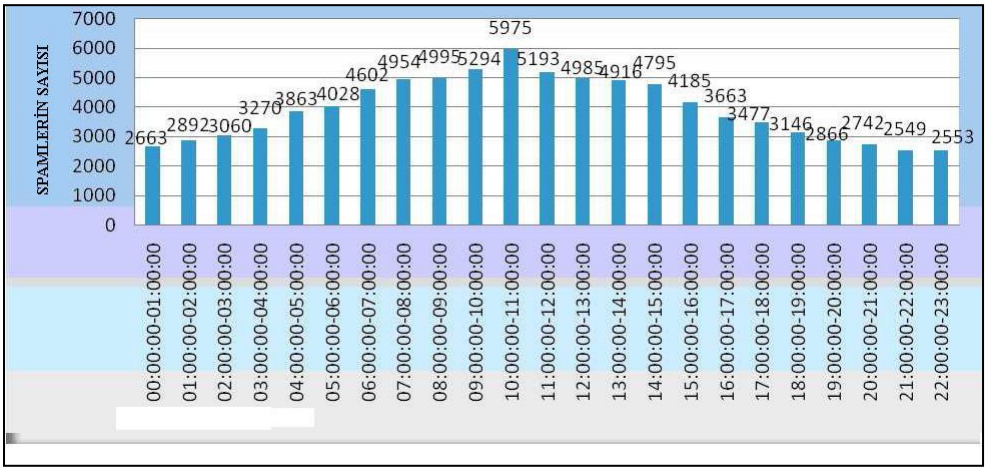
Şekil 4. İç mesaj logu için 1 saatte gelen spam maillerin toplam sayısı .



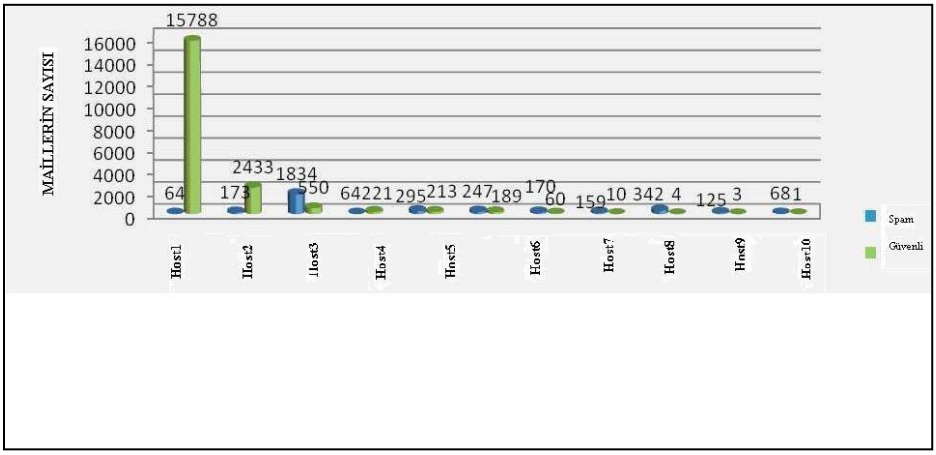
Şekil 5. İç mesaj logu için en meşgul 10 sunucu ve maillerin dağılımı.



Şekil 6. Dış mesaj logu için 1 saatte gelen güvenilir maillerin toplam sayısı .



Şekil 7. Dış mesaj logu için 1 saatte gelen spam maillerin toplam sayısı .



Şekil 8. İç mesaj logu için 1 saatte gelen spam maillerin toplam sayısı .

5. Kaynaklar

[1] Pathak A., Hu Y. C. and Mao Z. M.:Peeking into Spammer Behavior from a Unique Vantage Point. In: 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats, pp.????? (2008)

[2] Kanich C., Kreibich C., Levchenko K., Enright B., VoelkerG. M., Paxson V. And Savage S.: Spamalytics: An Empirical Analysis of Spam Marketing Conversion. In: 15th ACM Conference on Computer and Communications Security, pp. 3-14 (2008)

[3] Ramachandran A., Feamster N. and Dagon D.: Revealing Botnet Membership Using DNSBL Counter-Intelligence. In: SRUTI '06, pp. 49-54 (2006)

[4] Passerini E., Paleari R., Martignoni L. and Bruschi D.: FluXOR: detecting and monitoring fast-flux service networks; Emanuele Passerini. In: 5th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, pp. 186-206 (2008)

[5] Xie Y., Yu F., Achan K., Panigrahy R., Hulten G. and Osipkov I.:Spamming Botnets: Signatures and Characteristics. In: ACM SIGCOMM Computer Communication Review, pp. 171-182 (2008)

[6] Shah S. and Noble B. D.: A study of email patterns. In: SoftwarePractice and Experience, pp. 1515-1538 (2007)

[7] Leiba B., Ossher J., Rajan V. T., Segal R. and Wegman M.:SMTP Path Analysis. In: Conference on Email and Anti-Spam (2005)

[8] Rowe R., Creamer G., Stolfo S. J. and Hershkop S.: Behavior-based email analysis with application to spam detection. In: 9th WebKDD and 1st SNA-KDD 2007 Workshop on Web mMining and Social Network Analysis, pp. 109-117 (2007)