Ttnet'in SMTP Portunu Kapatmasını Doğru Okumak

Internet dünyasının en önemli sorunlarından biri SPAM konusudur. Eskiden bireysel olarak görülen spam aktiviteleri günümüzde başlı başına ticari bir sektör olmuş durumda. Öyle ki spam göndermek için ISP'lerle anlaşanlar, hatta sadece Spam gönderimi için ISP kuranlara bile rastlıyoruz.

Spam'in en önemli kaynağı zombi denilen ele geçirilmiş ve çeşitli amaçlarla yönetilen sistemlerdir. Bu tip sistemler işletim sistemlerinde çıkan çeşitli güvenlik açıklıkları kullanılarak ele geçirilmiş ve merkezi yönetime sokulmuş hizmetkar sistemlerdir. Dünyadaki spam gönderici networkler incelendiğinde zombilerin kullanıldığı kolaylıka görülebilir.

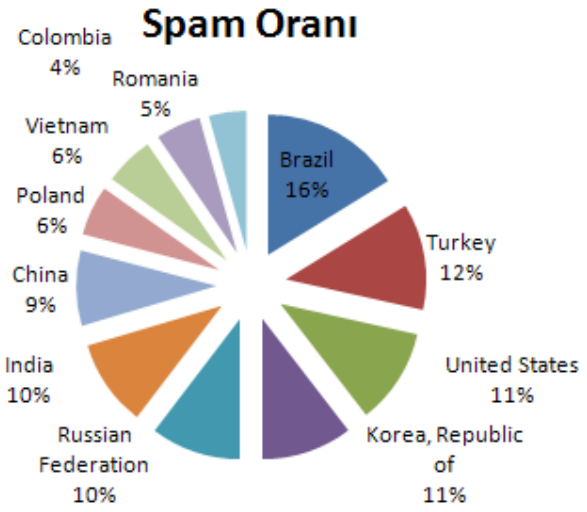
Türkiye Spam Servisleri Konusunda Nerede?

Bağımsız Spam takip kuruluşlarından Spamhaus'un güncel sonuçlarına göre TTNet dünyada en fazla spam gönderen dördüncü network'e sahip.

The 10 Worst Spam Service ISPs		As at 25 April 2009
Rank	Network	Number of Current Known Spam Issues
1	covad.com	41
2	vsnlinternational.com	33
3	tiscali.it	32
4	ttnet.net.tr	30
5	relianceglobalcom.com	29
6	hostway.com	28
7	gilat.net	27
8	tbroad.com	26
9	ovh.net	26
10	sprint.net	26

Bunun temel sebebi TTNet'den hizmet alarak internete bağlanan bilgisayarların güvenlik açısından zayıf olması ve çoğunun zombi ordusuna dahil edilmiş olması.

Geçtiğimiz Nisan ayı içerisinde yabancı araştırma kaynaklarını doğrular nitelikte bir çalışma da Türkiye'de yapıldı. Günde ortalama 600.000 spam alan bir sistem üzerinde yaptığımız araştırma bize benzer sonuçları verdi. Malesef ki Türkiye spam gönderen listenin ikinci sırasında.



TTNet'den Spam'e Çözüm Önerisi

TTNet'in bu durumunu değerlendiren yetkililer dünyadaki spam engelleme yöntemlerini araştırarak Türkiye için en uygun ve hızlı çözümün STMP portunun kapatılması, mail gönderim işleminin daha güvenli olan submission(TCP/587) portu üzerinden yapılması olduğuna karar vermiş. Bu yöntemi uygulamadan önce çeşitli ISP'ler ile defalarca görüşüldüğü ve yan etkilerinin neler olabileceği konusunda tartışıldığını düşünüyorum.

Ttnet yapılacak bu çalışmayı Şimdi E-posta Kutunuz Daha Güvenli! Parolası ile duyurdu. Çalışmanın sayfası oldukça bilgilendirici fakat asıl can alıcı nokta konusunda herhangi bir bilgi yok. Yani 25. Portu kapatıp yerine 587.portu açmak gerçekte ne işe yarayacak? Durum böyle olunca yapılan bu çalışma daha çok sansür ve özgürlükler bağlamında ele alınıyor. Internette yaptığım kısa bir araştırma sonrasında TTNet'in yapmaya çalıştığının anlaşılmadığını gördüm.

Bu yazı kısaca Ttnet'in seçtiği bu yöntemin neden etkili olabileceğini teknik olarak açıklamak için hazırlanmıştır.

Ttnet Tam Olarak Ne Yapıyor?

Proje kapsamında dinamik IP'li ADSL abonelerinin tcp/25(SMTP) portu dış dünyaya kapatılacak. Bunun yerine mail gönderim işleminin 587(submission) portu üzerinden yapılması isteniyor.

Ilk bakışta akla port değiştirmek neyi çözer ki gibi bir düşünce geliyor. SMTP portu 25 ile Submission portu 587 arasındaki fark bilinirse aslında bu yöntemin spamlerin azaltılması yönündeki gerçek etkisi anlaşılır. Aslında keramet port da değil port üzerinde çalışacak olan uygulamada.

SMTP Nasıl Çalışır, Submission SMTP'ye Ne Sağlar?

Bir SMTP sunucu iki tür hizmet verir; a)Kullanıcıların mail göndermesi , b)Başka mail sunuculardan gelen mailleri kabul etmek .

Benzer şekilde SMTP sunucular kendilerine gelen bir mail üzerinde iki tür işlem yapabilirler

1)Gönderilen mail domaini sistemde tanımlı ise kabul ederler.
2)Gönderilen mail domaini sistemde tanımlı değilse hata dönerler.

Bir de sistemin relaya açık olma durumu vardır ki bu durumda mailin nerden nereye gönerildiğine bakılmaksızın işlem yapılır. *Spamciler için bu tip sunucular hazine değerindedir.*

Sıkı yapılandırılmış bir mail sunucuda kayıtlı kullanıcılar mail gönderebilmek icin SMTP AUTH(kimlik dogrulama) yöntemini kullanır. Böylece kullanıcı kendisini sisteme tanıtarak istediği yere mail gönderebilir. *Bu yöntem spamı önlemede en etkin çözümdür*.

Mail sunucu yazılımlarında smtp-auth(kimlik doğrulama) özelliği isteğe bağlı olarak aktif edilir(helo/ehlo komutlarıyla). Dolayısı ile smtp portu üzerinden hem normal kullanıcılar mail gönderme işlemi yapar hem de internetteki diğer smtp sunucuları bağlantı kurarak mail bırakır.

Eğer 25 smtp portu üzerinden zorunlu smtp auth yaptırırsak internet üzerindeki mail sunuculardan mail almak imkansız hale gelir.

İşte burada Submission yardımımıza koşuyor. SMTP'den ayrı bir porttan yine smtp protokolünü destekleyen fakat zorunlu smtp-auth isteyen bir servis çalıştırıyoruz(qmail, postfix, exim vs) ve bu porttan bağlanan kullanıcı mail göndermeden önce mutlaka kendisini tanıtması gerekiyor.

Bu yöntemi kullanan TTNet de 25. portu kapatarak adsl abonelerinden –kendilerinin haberi olmadan-yayılacak spamleri engelliyor. Kullanıcılar SMTP ayarlarını değiştirip mail gönderim işlemini 587. port üzerinden yapacağı için mail gönderimlerinde problem çıkmayacaktır.

Peki submission portunu kullanmaya başlayınca sadece port mu degisecek?

Hayır! Submission , SMTP portundan farklı olarak kendisine bağlanan her kullacıdan zorunlu smtp auth –kendilerinin sistemde tanımlı olduklarını kanıtlamaları- isteyecektir.

Böylece 587 uzerinden sadece mail sunucularda tanımlı kullanıcılar mail gönderebilecek. Spam gondermek isteyen kişiler ilgili sistemde tanımlı değilse mail gönderemeyecekler. Ek olarak worm vs bulaşmış sistemler dışarı doğru SMTP bağlantısı açamayacağından spam gönderemeyecekler.

Yani sistemde iki tane smtp portu açılmış olacak. Bunlardan biri(TCP/25) dışardan mail alımları için(yahoo, hotmail ve diger mail sunucular)digeri (TCP/587)de ADSL abonelerinin mail gondermesi için zorunluy smtp auth gerektirecek bir port.

Bu Yöntem Türkiye Dışından Gelen Spam Mailleri de Engelleyecek mi?

Hayır, zira dışardan gelen spamler yine 25. porttan gelecekler. Ama amaç zaten dışardan gelen spamleri kesmek degil, TTnet'den spam gonderilmesini engellemek.

Firewall'dan 587. portumu 25. porta yönlendirsem çözüm olur mu?

Evet, kısa vadede bir çözüm olur. Hayır, spamciler size 25. porttan değil de 587. porttan mail gönderebilirler. Dolayısıyla 587. portu 25. porta yönlendirmek yerine 25. portta normal smtp servisi 587. portta submission özelliği olan(zorunlu smtp auth gerektiren)mail sunucu yazılımı çalıştırılmalı.

Bizden başka bu yöntemi uygulayıp başarılı olan var mı?

Kullanılan yöntem Ttnet'in kendi uydurduğu, bulduğu bir yöntem değil.Tüm dünyada spamle başı dertte olan ISP'lerin uzun zamandır(bazıları yeni yeni geçiş yapıyor)kullandığı bir yöntem.

Dünyanın sayılı büyük ISP'lerinden Verizon, spam gönderenler listesinde ilk sırada yer alırdı. Bu çalışma(ve başka ek çalışmalar) sonrasında ilk 10 da gözükmemeye başladı.

Statik IP Adresimde Mail sunucu Çalışıyor Etkilenecek miyim?

Statik IP Adresi kullananlar bu yapılandırmadan etkilenmeyecekler.

Qmail mail sunucu yazılımı için submission ayarları.

Qmail kullanıyorsanız Spamdyke yazılımını kullanarak submission özelliğini devreye alabilirsiniz

Notlar:

Submission hakkinda detayli bilgi için RFC'si incelenebilir http://www.ietf.org/rfc/rfc2476.txt

Yazar: Huzeyfe ÖNAL huzeyfe@lifeoverip.net

http://www.lifeoverip.net