

Spam nedir, nasıl önlem alınır ?

Bildiğiniz gibi günümüzde insanlara ulaşabilmenin en kolay, hızlı ve ucuz yolu e-mail.

Biz nasıl müşterilerimize veya kullanıcılarımıza e-mail yoluyla ulaşmak, bilgilendirmek istiyorsak; phishing yapanlar da aynı yöntemle kendi maillerini milyonlarca kişiye ulaştırmaya çalışıyorlar.

Aslında ucuz ve zahmetsiz gibi görünen bu işlem phishing yapanlar için büyük masraf çünkü yaptıkları işlem yasal olmadığı için sürekli yeni dedicated, yeni ip adresleri kiralamak zorundalar amaçları bu işi ücretsiz yapmak olduğu için de ortaya maaliyetsiz sunucu ihtiyacı çıkıyor.

Spamı sadece phishing yapanlar değil, porno, finans, seyahat sektörü vs.. bir sürü amaçla bu işlem gerçekleştirilmekte.

Siz sayısı onu geçmeyen müşterilerinize bile e-mail ile ulaşırken sıkıntı çekerken, onlar nasılmilyonlarca kişiye ulaşıyor bunu merak ediyorsanız yazının devamı ilginizi çekebilir.

Kullanıcıya bir e-mail gönderildiğinde, e-maili alan sunucu: üzerindeki yazılıma bağlı olarak bazı testlerden geçirir. İlgili maili gönderen sunucu kara listede (blacklist) kayıtlı mı, gönderdiği e-mail kişiye özel mail mi yoksa toplu mail mi, gönderdiği mailin içerisinde yer alan kodlar alıcının veri güvenliğini tehdit edecek zararlı yazılımlar mı yoksa tamamen yasal ve yararlı bir içerik mi vs.. Bu süzgeçlerden geçtikten sonra da alıcının filtresine göre gelen kutusuna veya spam kutusuna gönderilir.

Spam işlemini gerçekleştiren kişiler de (spamer) aşağı yukarı spam filtrelerinin çalışma prensibini bildiklerinden dolayı olayın içerik kısmını ellerinden geldiği kadar kusursuz yapıp, blacklistte olmayan sunuculardan, ip adreslerinden e-mail göndermeye çalışıyorlar.

Peki başkalarının sunucularından email göndermek bu kadar kolay mı ?

Aslında kolay fakat problem şu ki siz istediğiniz kişinin adından mail gönderseniz de o mail alıcının gelen kutusuna düşmeme ihtimali yüksek çünkü günümüzde spam filtrelerinin çoğunda gönderilen mailin smtp server ile oturum açıp mı gerçekleştirildiğini kontrol ediyor. Oturum açılarak gönderilmişse doğal olarak spam skoru düşüyor, oturum açılmamışsa da spam skoru yani spam olma ihtimali artıyor.

Peki bu durumda spamerlar nasıl oluyor da başkalarının sunucularında oturum açıp, o sunuculardan mail gönderebiliyor ?

Bu tamamen sizin sunucunuzun kullandığı yazılımlarla, seçtiğiniz şifrelerle ilgili bir durum. Örneğin sunucunuzda kullandığınız mail, ftp gibi yazılımlarda herhangi bir bug olması durumunda sunucunuza o yazılımın açığı kullanılarak erişilip, sunucunuzdan bambaşka mail adresleri ile, mailler gönderilebilmekte.

Buna alınacak önlemler neler ?

Öncelikle "en güvenli sistemin fişi çekik sistem" olduğunu hatırlatıp, sunucunuzda her zaman kullandığınız yazılımların en güncel versiyonlarını kullanmanızı, günlük, haftalık periyotlarla sunucunuzda kullandığınız mail yazılımının giden kutusundaki mail sayısına, şüpheli maillere bakmanız gerekmekte. Herhangi bir olumsuzluk durumunda anında sorunun nedenini tespit edip, müdahale etmeniz gerekmekte aksi taktirde bir süre sonra spamerlar sizin sunucunuzu IP adresiniz blackliste girdiği için bırakacağı gibi, sizin gönderdiğiniz mailler de blacklistte gözükeceğinden dolayı mailleriniz alıcılara ulaşmayacaktır.

Peki blacklist nedir ?

Spam filtreleri IP adresinin spam yapıp yapmadığını öğrenebilmek için bir veritabanına ihtiyaç duyar. İnternette ise barracuda, spamcop gibi onlarca firma kendilerine yapılan şikayet, bilgilendirmeler vs.. sayesinde bu IP veritabanlarını kullanıcılara sunmaktadır. Spam filtreniz size bir mail geldiğinde, gönderen sunucunun IP adresini bu sunucularda tarar ve sonuca göre maili ilgili klasöre yönlendirir.

Peki blacklistte olup, olmadığımı nereden anlayabilirim ?

Gönderdiğiniz maillere gelen otomatik cevaplardan anlayabileceğiniz gibi online araçlarla IP adresinizi çoklu olarak sorgulayabilirsiniz. Bu konuda başarılı bulduğum ve sevdiğim, önerdiğim araç ise mxtoolbox'ın aracı. [buradan](https://mxtoolbox.com/blacklists.aspx) kendi ip adresinizi veya domaininizi yazarak otomatik olarak blacklistte olup, olmadığınızı sorgulayabilirsiniz.

IP adresim blackliste eklenmiş ne yapmalıyım ?

Burada yapmanız gereken işlem oldukça basit. Öncelikle neden IP adresinizin blackliste eklendiğini bulmanız gerekmekte. Bunun için elinizde herhangi bir kayıt veya bilgi yoksa yapmanız gereken ilk işlem sunucunuzda tarama yapıp, mail gidip gitmediğini, gidiyorsa nasıl/neden gittiğini bulup bunu çözmek. Bunu çözdükten sonra da IP adresinizin blackliste kayıtlı olduğu firmanın internet sitesine

girerek, sitedeki yönergeleri izleyerek ne problem yaşadığınızı ve problemi nasıl çözdüğünüzü açıklayan bir yazı yazmanız durumunda 24-48 saat içerisinde IP adresinizi blacklistten çıkartıyorlar. Çıkarttıktan sonra da bir ay içerisinde aynı spam mailler devam ederse blackliste tekrar alınıyorsunuz ve firmaya bağlı olarak blacklistten kurtulma süreniz doğal olarak uzuyor.

Mustafa Erdinç ZORBA

28 Oca. 2014

info@merdincz.com

www.merdincz.com