

E-POSTA GÖNDERİCİLERİNİN TESPİTİ

Burak DAYIOĞLU, dayioglu@metu.edu.tr

1. E-posta Hizmetlerinde Problemler

E-posta hizmetleri için kullandığımız SMTP (Simple Mail Transfer Protocol) protokolü İnternet'in ilk günlerinde tasarlanmış, o günlerin şartları ve ihtiyaçları doğrultusunda şekillendirilmiştir. Ne yazık ki, İnternet ilk günlerindeki o güven dolu ortamdan çok uzaklaştı ve artık İnternet kullanımı pek çok güvenlik tehdidini de beraberinde getiriyor.

SMTP protokolünün gönderici bilgisayarlara olan gereksiz güveni sayesinde bugün herkesin başka bir adresten geliyormuşçasına e-posta mesajları gönderebilmesi mümkün hale gelmiştir; bir iş arkadaşınıza patronunuzdan geliyormuş gibi görünen bir e-posta göndermeniz kolayca mümkündür. Bu nedenle e-posta mesajları, elektronik ortamda imzalanamadığı sürece *çok önemli işler için kullanılması riskli* olarak nitelendirilebilir. Bu problemi çözmek üzere PGP ve S/MIME sayısal sertifika düzeneklerinden faydalanılabilir.

Giderek artan bir biçimde yaygınlaşan Hotmail, Yahoo, HushMail gibi hizmetler, isteyenlerin kimliklerini gizleyebileceği bir biçimde e-posta gönderip alabilmesini mümkün kılmaktadır. Çok kısa sürede ve denetimsiz biçimde edinebileceğiniz bir e-posta adresi ile bir iş arkadaşınıza rahatsız edici tatsız mesajlar gönderebilir ve bunu yaparken kimliğinizi de gizleyebilirsiniz.

Kimliği gizlemeye yönelik bu iki faaliyetin fazlası ile kolay bir biçimde gerçekleştirilebilmesinin bir sonucu olarak e-posta, taciz ve tehdit için telefon ve postanın yerini almaya başlamıştır.

E-posta mesajlarının göndericilerinin tespit edilmesi sanıldığı gibi imkansız değildir; belirli durumlarda fazlası ile kolay bile olabilir. Önemli olan göndericinin IP adresinin tespit edilmesidir; IP adresi tespit edildikten sonra bu adrese sahip kurum ile temasa geçilerek göndericinin gerçek kimliği edinilebilir.

2. Mesaj Başlıklarının İncelenmesi

Bir mesajın incelenmesinin ilk adımı mesaj başlığının incelenmesi olmalıdır; mesaj başlığında aradığımız mesajın göndericisi bilgisayarın IP adresi ya da mesajı ilk teslim alan bilgisayarın IP adresidir. Aşağıda örnek bir mesaj tüm başlıkları görünecek biçimde verilmiştir:

```
Return-Path: <palyaco@dayioglu.net>

Received: from myra.cc.metu.edu.tr (myra.cc.metu.edu.tr
[144.122.199.93]) by knidos.cc.metu.edu.tr (8.11.6/8.11.6) with
ESMTP id g1HEdd095784 for <dayioglu@metu.edu.tr>; Sun, 17 Feb 2002
16:39:40 +0200

Received: from larva.cc.metu.edu.tr (larva.cc.metu.edu.tr
[144.122.202.144]) by myra.cc.metu.edu.tr (8.11.6/8.11.6) with SMTP
id g1HEcOf16298 for dayioglu@metu.edu.tr; Sun, 17 Feb 2002 16:38:35
+0200 (EET)

Message-Id: <200202171438.g1HEcOf16298@myra.cc.metu.edu.tr>

Subject: acele para istiyorum!

From: Igrenc Palyaco <palyaco@dayioglu.net>

Date: Sun, 17 Feb 2002 16:38:35 +0200 (EET)

To: Burak <dayioglu@metu.edu.tr>

Bana acele $5000 vermezsen seni mahfederim, herseyi anlatirim...

-palyaco
```

Yukarıdaki mesajda Message-Id ve Received biçiminde verilen alanlar inceleme için büyük önem taşımaktadır. Message-Id alanı mesajı teslim alan ilk e-posta sunucu bilgisayarı tarafından atanan mesaj kimliğini göstermektedir. İnternet E-posta standardı gereği her mesaja atanan biricik bir kimlik bilgisi olmak zorundadır. Bir saldırgan bilinçli olarak bu alanı değiştirmek için çalışmadı ise bu alandaki bilgiye güvenebilirsiniz. Mesaj kimliği, mesajı teslim alan ilk e-posta sunucusunun adını ya da adresini de gözler önüne serecektir. Bu bilgi en azından mesajın hangi kuruluştan ya da hizmet sağlayıcıdan (İSS, Hotmail vb.) geldiğini anlamınızı sağlayacaktır.

Received biçiminde verilen alanlar, mesajın yol boyunca geçtiği tüm e-posta hizmet sunucularının bir kaydını içermektedir. Eğer bu kayıtların bir kısmı, yol üzerindeki bir posta sunucusu tarafından özellikle silinmediyse mesaj size ulaştırıldığında mesajın izlediği yolu detaylı bir biçimde görebilirsiniz. Yukarıdaki mesajda, ilk Received alanı saat 16:39:40'ta mesajın Myra bilgisayarı tarafından Knidos bilgisayarına verildiğini, ikinci Received alanı ise, saat 16:38:35'te mesajın Larva bilgisayarından Myra bilgisayarına verildiğini göstermektedir.

Mesajın alıcısı olan dayioglu@metu.edu.tr adresi ile ilişkili posta kutusunun Knidos bilgisayarı üzerinde olduğu, mesajın kronolojik olarak en son bu bilgisayar

tarafından alınmış olmasından anlaşılabilir. Mesajı ele alan kronolojik olarak en eski iletişim Larva ve Myra bilgisayarları arasında gerçekleşmişti, buradan mesajın Larva'dan çıkmış olabileceği sonucuna varabiliriz.

Bu noktada, mesajın en azından Larva'ya kadar geriye doğru takip edilmesini sağlamış olduk. Mesajın Larva'dan gönderilip gönderilmediğinden emin olmak için daha önce incelediğimiz Message-Id alanından edindiğimiz bilgiden faydalanacağız. Message-Id alanının, mesajı alan ilk e-posta sunucusu tarafından doldurulduğundan daha önce söz etmiştik. Mesaj kimliği ve mesajın izlediği yol ile ilgili olarak edindiğimiz iki bilgiyi birleştirdiğimizde mesajın Larva'dan gönderildiği sonucuna varabiliriz. Larva bilgisayarını, mesajın gönderildiği istemci bilgisayardır.

palyaco@dayioglu.net adresinden mesaj gönderen saldırgan, Larva bilgisayarını kullanmaktadır. Bu sonuç, elektronik ortamda gerçekleştirilebilecek incelemenin son noktasıdır. Daha ileri giderek Larva bilgisayarını kimin kullandığının bulunması (i) ya Larva bilgisayarına izinsiz bir girişi, (ii) ya da bürokratik bir süreç ile telefon/yazışma gibi iletişimi gerektirecektir.

3. Gelişmiş Yöntemler

Mesaj başlığı incelemesi, e-posta mesajlarının takip edilmesi ve gönderici IP adresinin (ve kullanıcısının) bulunması için her zaman yeterli olamayacaktır.

Web temelli posta arayüzleri (webmail, basilix, postaci, sqwebmail vb.) ya da web temelli hizmet sağlayıcılar (Hotmail, YahooMail vb.) kullanıldığında gönderici IP adresi mesaj başlığı içerisinde Received-By alanları arasında yer almayabilir.

Örneğin Basilix ve Hotmail, göndericinin IP adresini Received-By alanları arasında göstermemek ile birlikte, bu bilgileri mesaj başlığında adı X ile başlayan başka alanlarda göstermektedir. Yine de, göndericinin IP adresinin hiçbir biçimde başlık içerisinde yer almaması da mümkündür. Aşağıda gönderici ile ilgili alabildiğine sınırlı bilgi içeren bir örnek bir mesaj tüm başlıkları görünecek biçimde verilmiştir:

```
Return-Path: <burak@ucansupurge.org>

Received: from master.bedavamail.com ([192.142.105.7]) by
knidos.cc.metu.edu.tr (8.11.6/8.11.6) with ESMTTP id g1HFCAO102376
for <dayioglu@metu.edu.tr>; Sun, 17 Feb 2002 17:12:11 +0200

Received: (from root@localhost) by master.bedavamail.com
(8.11.6/8.11.6) id g1HFC3004989 for dayioglu@metu.edu.tr; Sun, 17
Feb 2002 17:12:03 +0200

Message-ID: <quirk.5b10139587233c6fc8431adc8@master.bedavamail.com>

Date: Sun, 17 Feb 2002 17:12:03 EET

From: Igrenc Paylaco <palyaco@bedavamail.com>

Subject: acele para istiyorum!

To: dayioglu@metu.edu.tr

Bana acele $1000 vermezsen seni mahfederim, herseyi anlatirim...

-p
```

Yukarıdaki mesajda, Received-By başlık alanları mesajın root@localhost kullanıcısından (ki bu kullanıcı master.bedavamail.com sisteminin bir kullanıcısıdır) gönderildiğini göstermektedir. Eğer master.bedavamail.com sisteminin root kullanıcısı bu mesajı göndermedi ise, yüksek ihtimalle bu mesaj, bu sistem üzerinden bir web arayüzü ile gönderilmiştir.

Göndericinin tespiti, mesaj başlıklarından gerçekleştirilememektedir. Bu durumda mesajı gönderen kişiye (Palyaço) okuması için hazırlanmış "özel mesajlar" göndererek adresini tespit etmeye çalışmak anlamlı olacaktır.

Özel mesajlar ile göndericinin kimliğinin tespiti için kullanılacak birden fazla farklı teknik söz konusudur. Bunlar, kısa açıklamaları ile aşağıdaki gibidir:

- ❑ **Özel resimler içeren HTML mesajların gönderilmesi:** Eğer palyaco@bedavamail.com HTML olarak biçimlendirilmiş mesajları HTML olarak görüntüleyerek okuyabiliyor ise, yalnızca bu kişi tarafından

görüntülenecek bir resimi sayfanın içine gömebilirsiniz. Size ait bir web sunucusuna yüklenecek bu resim için HTML içine gömülecek bir referans işinizi fazlası ile görecektir. Palyaço mesajı okuduğunda, e-posta istemcisi sizin web sitenizden ilgili resmi çekecek ve bu sayede IP adresi açığa çıkacaktır.

- **Javascript ya da VbScript içeren HTML mesajların gönderilmesi:** Javascript ya da VbScript çalıştırma becerisine sahip olan bir istemci ile belirlenen özel bir adresin ziyaret edilmesi sağlanabilir. Ziyaret edilen adresi taşıyan web sunucusunun kayıtları, Palyaço'nun IP adresini açığa çıkaracaktır.
- **Davet mesajı gönderilmesi:** Palyaço HTML mesaj okumayan/okuyamayan bir e-posta düzeneği kullanıyor ise, salt-metin biçiminde anlaşmalı bir web sitesindeki özel bir URL için "davet içeren" bir e-posta mesajı gönderilebilir. Palyaçonun ilgi alanına bağlı olarak, bir e-ticaret sitesinin özel bir promosyon duyurusu, bir spor sitesindeki çok çarpıcı yorumlara ilişkin bir haber ya da bir porno siteye kısıtlı süreli ücretsiz erişim ilk akla gelenler arasındadır. Yalnızca Palyaço tarafından ziyaret edilecek böylesi bir düzenek kurulduğunda, ziyareti gerçekleştiği anda IP adresi tespit edilebilir.

4. Özet ve Sonuç

E-posta mesajlarının göndericilerinin IP adreslerinin tespiti, pek çok durumda, yalnızca bireysel girişiminiz ile ve internet teknolojisinin sunduğu imkanları kullanarak gerçekleştirebileceğiniz bir faaliyettir. Pek çok durumda, mesaj başlıklarının incelenmesi göndericinin IP adresinin tespit edilmesine imkan verecektir.

Eğer mesaj başlıklarının incelenmesi sonuç vermiyor ise, IP adresi tespit edilmeye çalışılan kullanıcıya gönderilecek özel mesajlar ile adres tespitine çalışılabilir. Yalnızca takip edilen kullanıcı tarafından ziyaret edilecek bir web sayfası ya da görüntülenecek bir resmin sistem kayıtlarına ulaşılabilen bir web sunucu üzerine yüklenmesi anlamlı olacaktır.