



BİLGİ GÜVENLİĐİ
AKADEMİSİ
WWW.GUVENLIKEGITIMLERI.COM

Bilişim Suçlarında IP Adres Analizi

Adli Bilişim Açısından IP Adresleri

Huzeyfe ÖNAL

<huzeyfe@lifeoverip.net>

5/13/2010

[Son zamanlarda medyada geniş yer bulan çeşitli haberlerin ana temasını IP adresleri oluşturmaktadır. Bu yazı bilişim sistemleri kullanılarak işlenen suçlarda suçlunun kendini hangi imkanlarla nasıl gizleyebileceđi ve adli bilişim analizi yapanların IP adresleri konusunda nelere dikkat etmesi gerektiđi konularını ele almaktadır.]



İçerik Tablosu

Giriş.....	3
IP(Internet Protocol) Adresi.....	3
 IP adreslerini kim dağıtır?.....	4
 IP Adresi Neden Önemlidir?.....	4
 İstediğim IP adresini kullanabilir miyim?.....	4
 IP Adresi Sahibini Bulma.....	4
 IP Adresinin Ait Olduğu Ülkenin Bulunması.....	5
IP Spoofing Kavramı.....	5
 Başkasının IP Adresinden Nasıl Suç İşlenir?.....	5
DDoS Saldırılarında Kullanılan IP Adresleri.....	6
 Başka Ülkeden Geliyormuş Gibi E-posta Göndermek.....	6
Ücretsiz Anonim Proxy Hizmetleri.....	6
 İstenilen Ülkeden IP Adresi Kullanma.....	6
Sonuç.....	8

Giriş

Günümüz modern insanının hayatı iki farklı dünyadan oluşmaktadır. Bu dünyalardan biri fiziksel olarak yaşadığımız sosyal hayatımız diğeri de en az sosyal hayat kadar vakit geçirdiğimiz ve bağımlı olduğumuz siber dünyadır.

Siber dünyanın sunduğu olanaklar arttıkça, gerçek hayattaki bir çok işlev siber/sanal versiyonuyla yer değiştirmektedir ki bu da insanların siber dünyaya daha fazla bağımlı olmasına sebep olmaktadır. Siber dünya kavramı detaylı olarak incelenirse bu dünyanın iki farklı profilde insanlara olanak sağladığı ortaya çıkacaktır. Profillerden biri işlerini daha rahat yapabilmek için siber dünyanın olanaklarını kullanan masum vatandaş, diğeri de bu dünyayı kötü amaçlı kullanmak isteyen suç şebekeleri.

2000'li yıllardan itibaren işlenen suçlar yakından incelenirse siber dünyanın -dolayısıyla da bilişimin- suç örgütleri tarafından ciddi bir şekilde kullanıldığı görülecektir. Siber dünya denildiğinde ise akla ilk gelen bileşen Internetin de temel yapıtaşlarından biri olan IP adresleridir.

Bu yazıda bilişim suçlarında IP adreslerinin yeri ve önemi anlatılmaktadır.

IP(Internet Protocol) Adresi

Teknik olarak IP adresi, bir ağa bağlı cihazların birbirleriyle haberleşebilmesi için gerekli adrestir. Internet de ağları birbine bağlayan en büyük ağ olduğu için internete bağlı her bilgisayar bir IP adresine sahip olmalıdır. Her ne kadar internet ortamında isimler kullanılsa da (alan adları) bilgisayarlar haberleşme için isimleri IP adreslerine çevirmektedir. Internete siber dünya olarak bakarsak IP, siber dünyada bizi adresleyen bir numaradır diyebiliriz.

Gerçek hayatta nasıl adresler tanımlanırken mahalle, sokak, ilçe, il şeklinde tanımlanıyorsa sanal dünyada da IP adresleri benzer şekilde tanımlanmaktadır.

Bilişim Suçlarında IP Adres Analizi

IP adreslerini kim dağıtır?

IP adresleri IANA başkanlığında RIR(Regional Internet Registry) olarak adlandırılan organizasyonlar tarafından dağıtılır. Tüm dünyaya IP dağıtan beş farklı RIR vardır. Bunlar bölgelere göre IP dağıtım işlemlerini üstlenmişlerdir.

Sıradan Internet kullanıcılarına(son kullanıcılara) IP dağıtım işlemi hizmet aldıkları ISS(Internet servis sağlayıcısı)tarafından yapılır. Bazı ISS'ler sabit IP adresi verebilirken bazı ISS'ler değişken IP adresi ataması yapar.

IP Adresi Neden Önemlidir?

Siber dünyada bizleri tanımlayan ayırt edici en önemli özellik IP adreslerimizdir. Gerçek dünyadaki adreslerimizden farklı olarak siber dünyada IP adreslerimiz kimliğimizdir. Bunun sebebi siber dünyada yapılan her işlemde IP adreslerinin kullanılması ve ötesinde IP adres kullanılarak yapılan her tür işlemde IP adresinin sahibinin sorumlu olmasıdır.

İstediğim IP adresini kullanabilir miyim?

IP adresleri belirli bir hiyerarşi ve sisteme göre dağıtılır ve dağıtılan IP adresleri omurga yönlendiriciler tarafından yönlendirilir. Dolayısıyla isteyen istediği IP adresini kullanamaz.

Bir IP adresinin kime, hangi kuruma ait olduğu RIR'ler üzerinden yapılacak sorgulamalarla belirlenebilir. Bu sorgulamalara "whois" adı verilir. Genellikle IP adresleri kurumlara verilir ve kurumda birileri IP adresinin alım işlemlerinden sorumlu olur, whois sorgularında çıkan adresler genellikle IP adresleriyle ilgili bir sorun/talep olduğunda ulaşılabilir için verilir.

Bilişim Suçlarında IP Adres Analizi

Query the RIPE Database

Search for Search

By pressing the "Search" button you explicitly express your agreement with the [RIPE Database Terms](#)

[Advanced Search Form](#)

[Switch to the RIPE TEST Database](#)

```
# This is the RIPE Database query service.
# The objects are in RPSL format.
#
# The RIPE Database is subject to Terms and Conditions.
# See http://www.ripe.net/db/support/db-terms-conditions.pdf
#
# Note: This output has been filtered.
#       To receive output for a database update, use the "-B" flag.
#
# Information related to '91.93.0.0 - 91.93.255.255'

inetnum:          91.93.0.0 - 91.93.255.255
netname:          IR-TELETEK-20060824
descr:           Global İletişim Hizmetleri A.S
country:         TR
org:             ORG-GIHA1-RIPE
admin-c:         OC928-RIPE
tech-c:          OC928-RIPE
status:          ALLOCATED PA
mnt-by:          RIPE-NCC-HM-MNT
mnt-lower:       MNT-TELETEK
mnt-routes:      MNT-TELETEK
source:          RIPE # Filtered

organisation:    ORG-GIHA1-RIPE
org-name:        Global İletişim Hizmetleri A.S.
org-type:        LIR
address:         Global İletişim A.S
                 Network Admin
                 Ayazmadere Caddesi.Aksit Plaza. 12/1
                 Fulya/Besiktas
                 34349 ISTANBUL
                 TURKEY
phone:           +90 212 227 70 30
fax-no:          +90 212 227 87 00
-mail:           netadmin@teletek.net
```

Sorgulanan IP adresine ait
sorumlu kurum/kişi bilgileri.

Sorgulanan bir IP adresine ait kurum/kişi bilgileri

IP Adresi Sahibini Bulma

Yapılan whois sorgusunda IP adresinin hangi kuruma ait olduğu ortaya çıkacaktır. Buradaki kurum bilgilerini kullanarak IP adresinin gerçek sahibi bulunabilir.

İnternet servis sağlayıcılar 5651 sayılı kanun gereği internet hizmeti verdikleri tüm kullanıcılara ait erişim bilgilerini tutmakla yükümlüdürler. Kanun erişim bilgisini aşağıdaki gibi tanımlamaktadır:

Erişim sağlayıcı trafik bilgisi: İnternet ortamına erişime ilişkin olarak abonenin adı, adı ve soyadı, adresi, telefon numarası, abone başlangıç tarihi, abone iptal tarihi, sisteme bağlantı tarih ve saat bilgisi, sistemden çıkış tarih ve saat bilgisi, ilgili bağlantı için verilen IP adresi ve bağlantı noktaları gibi bilgiler

BILGI GUVENLIGI AKADEMISI | www.guvenlikegitimleri.com

Bilişim Suçlarında IP Adres Analizi

Erişim sağlayıcı trafik bilgisi: İnternet ortamına erişime ilişkin olarak abonenin adı, adı ve soyadı, adresi, telefon numarası, abone başlangıç tarihi, abone iptal tarihi, sisteme bağlantı tarih ve saat bilgisi, sistemden çıkış tarih ve saat bilgisi, ilgili bağlantı için verilen IP adresi ve bağlantı noktaları gibi bilgileri,

Tanımdan da anlaşılacağı üzere Türkiye içerisinde bir IP adresine ait sorumlular belirlenebilir.

IP adresi Türkiye harici bir ülkeye aitse bu durumda yasal yollardan talep yapılarak ilgili ülkeden IP adresi sahibi bilgileri istenebilir fakat IP bilgileri istenen ülkenin kanunlarına göre bu bilgiyi almak kolay olmayabilir.

IP Adresinin Ait Olduğu Ülkenin Bulunması

IP adresleri dağıtılırken sistematik ve hiyerarşik bir yapı kullanıldığını belirtmiştik. Bu sistematik yapıda IP adreslerinin hangi ülkeye ait olduğu bilgisi rahatlıkla bulunabilir.

Google üzerinden “geo ip” “country ip blocks” anahtar kelimeleriyle yapılacak aramalarda bir ip adresinin hangi ülkeye ait olduğu bilgisi edinilebilir.

Bir IP adresinin hangi ülkeye ait olduğu bilgisi

IP Spoofing Kavramı

İnternetin çalışmasını sağlayan TCP/IP protokol ailesi geliştirilirken güvenlik temel amaç olmadığı için olabildiğince esnek davranılmıştır. Bu esneklik IP adreslerinin aldatılabilir(spoofed) olmasını sağlamıştır. Ip spoofing yaparak başkasının IP adresinden istenilen internet aktivitesi yapılabilir.

Son yazdığımız cümle bundan on sene öncesi için geçerli olsa da günümüzde pratik olarak geçersizdir. Bunun temel nedeni günümüz modern işletim sistemlerinin protokoldeki eksik noktalara kalıcı çözüm getirmeleridir.

Özellikle internetde en sık kullanılan HTTP, SMTP, HTTPS gibi protokollerin temelinde bulunan TCP(TCP/IP protokol ailesinden) bu tip sahtecilik işlemlerini engelleme amaçlı bir yöntem kullanır.

Bilişim Suçlarında IP Adres Analizi

Bu yöntem kısaca 3 way handshake olarak adlandırılır ve kullanıcı bir işlem yapmadan önce kullanıcı ile sunucu bilgisayarları arasında bir iletişim kanalı kurulmasını sağlar. Bu iletişim kanalının kurulmasında kullanılan bazı parametrelere (ISN numaraları) günümüz işletim sistemlerinde oldukça güçlü olduğu için IP spoofing yapılamaz.

Kısacası TCP kullanan uygulamalarda(web sayfalarını gezerken, e-posta gönderirken, bankacılık işlemleri yaparken) teorik olarak IP spoofing mümkün olsa da pratik olarak mümkün gözükmemektedir.

Bununla birlikte DNS gibi UDP kullanan uygulamalarda IP spoofing yapmak hala mümkündür.

Başkasının IP Adresinden Nasıl Suç İşlenir?

Kısaca yukarıda bahsettiğimiz IP spoofing işlemi kullanılarak istenen herhangi birinin IP adresinden ciddi suçlar işlenemez ancak aşağıdaki durumlar oluşursa istenilen IP adresinden suç işlenebilir:

- IP adresini kullanan bilgisayardaki güvenlik açıklıkları kullanılarak ajan yazılımlar yüklenir ve bu yazılımlar kullanılarak IP Adresinden geliyormuş gibi suç işlenebilir.
- IP adresi eğer NAT yapılan bir IP ise ilgili ağda bulunan herhangi birinin makinesine bulaştırılacak ajan yazılımlar sayesinde IP adresi kullanılarak suç işlenebilir
- IP adresi eğer aynı zamanda kablosuz ağa sahipse bu kablosuz ağa sızılarak IP adresinden suç işlenebilir

Yukarıda sayılan maddeler oluşmasa bile IP adresiniz DoS saldırılarında sizden habersiz kullanılabilir.

DDoS Saldırılarında Kullanılan IP Adresleri

DDoS saldırıları herhangi bir sistemi çalışamaz hale getirmek için yapılan saldırılardır. Bu tip saldırılar genellikle binlerce farklı bilgisayar kullanılarak yapılır ve hedef sistemin kapasitesinin kaldıramayacağı kadar trafik gönderilir.

BİLGİ GÜVENLİĞİ AKADEMİSİ | www.guvenlikegitimleri.com

Bilişim Suçlarında IP Adres Analizi

DDoS saldırılarında tercih edilen yöntemlere göre IP adresi spoof işlemi gerçekleştirilebilir. Eğer yapılan saldırı SYN Flood, UDP flood tarzıysa saldırgan oturduğu yerden istediği IP adresini spoof ederek saldırı gerçekleştirebilir.

Bu da çeşitli durumlarda iki firmayı gereksiz yere karşı karşıya getirebilir. Mesela X firmasından aldığı üründen memnun kalmayan saldırgan internette ücretsiz edinebileceği basit araçlarla X firmasının rakibi olan Y firmasına sanki X firmasından geliyormuşçasına DoS saldırısı gerçekleştirebilir. Y firması güvenlik sistemlerinde analiz yapıldığında saldırının X sisteminden geldiği düşünülecektir.

Yine benzeri şekilde zombi sistemler kullanılarak yapılan DDoS saldırılarında kullanılan IP adresleri gerçek olsalar bile sahibinin haberi olmadan sisteme yüklenen zararlı yazılımlarla gerçekleştirildiği için asıl faili bulmak oldukça zor olacaktır.

Başka Ülkeden Geliyormuş Gibi E-posta Göndermek

Ultrasurf, TOR gibi trafik anonimleştirme yazılımları kullanılarak yapılan işlemlerin farklı ülkelerden geliyormuş gibi gözükmesi sağlanabilir. E-posta kullanımında sık kullanılan iki yöntem vardır: bunlardan biri webmail hizmeti kullanmak (Hotmail, Yahoo gibi servislerin kullanımı) diğeri de Microsoft Outlook, Mozilla Thunderbird gibi e-posta istemcisi kullanmaktır. Her iki yöntemde de proxyler aracılığıyla trafik istenilen ülkeden geliyormuş gibi gösterilebilir fakat istenilen IP adresinden geliyormuş gibi gösterilemez.

Ultrasurf kullanılarak yapılan bir web sayfası ziyaretinde gözüken IP adresi bilgisi

Gönderilen e-postanın başlık bilgileri incelenirse e-posta sahte dahi olsa nereden gönderildiği bilgisi edinilebilir.

Ücretsiz Anonim Proxy Hizmetleri

İnternet üzerinde hizmet veren binlerce ücretsiz anonim proxy hizmeti bulunmaktadır.

Bu hizmetlerden bazıları ülke bazında

BİLGİ GÜVENLİĞİ AKADEMİSİ | www.guvenlikegitimleri.com

Bilişim Suçlarında IP Adres Analizi

özelleştirilmiş hizmet sunmaktadır. Yani proxy servisini kullanırken hangi ülkeden çıkış yapılacağı belirtilerek tüm trafiğin ilgili ülkeden çıkması ve sunucularda o ülkeden geliyormuş gibi gösterilmesi sağlanabilir.

İstenilen Ülkeden IP Adresi Kullanma

Aşağıdaki ekran görüntüsü proxylerden ülke olarak Kanada'nın seçilmesi sonrası alınmıştır.

Bu proxy kullanılarak yapılacak bir işlemde asıl faili bulmak oldukça zordur. Bunun temel nedeni internet üzerinde aktif çalışan binlerce proxy servisinin hangi kullanıcının hangi zaman diliminde nereye bağlandığı bilgisini tutmamasıdır.

Sonuç

İnternet altyapısı kullanılarak işlenen suçlarda şüpheli davranılmalıdır. Ele geçirilen bir IP adresinden yola çıkarak yapılacak işlemler işi tezgahlayan kişi tarafından bilindiğinden dolayı işe yaramayacaktır. Hatta özellikle yabancı IP adresleri kullanılarak belirli kişi/kurumlar töhmet altında bırakılmak istenebilir.

Bu gibi durumlarda suçluyu bulmak gerçek hayata göre daha zor görünse de konusunun uzmanı bir adli bilişimci suçlunun nereden geldiğini, kendisini gizleyip gizlemediğini, gizlediyse hangi yöntemleri, araçları kullanarak gizlediğini ortaya çıkarabilir.

İnternetin temel yapıtaşı olan TCP/IP protokolü ve bu protocol ailesine ait güvenlik risklerini uygulamalı olarak öğrenmek için “Uygulamalı TCP/IP Güvenliği Eğitimi”ne kayıt yaptırabilirsiniz.

(<http://www.guvenlikegitimleri.com/?p=1160>)