

# IPv6 Ağlarında Solucan Dağılımı

Onur Bektaş<sup>1</sup>

Murat Soysal<sup>2</sup>

Ağ Teknolojileri Birimi  
TÜBİTAK ULAKBİM, ANKARA

<sup>1</sup>e-posta: onur@ulakbim.gov.tr

<sup>2</sup>e-posta: msoysal@ulakbim.gov.tr

## Özet

Günümüzde internetin sağladığı her noktadan ağa bağlanma kolaylığı, ağa bağlanan cihazların sayısının ve çeşitliğinin bant genişliği ile artması, internet solucanları için çok elverişli koşullar sağlamaktadır. Bu makalede solucanların yayılma yöntemleri, IPv6 ağlarında solucan yayılımının IPv4 ağlarından farkları, solucan dağılımının IPv6 ağlarında nasıl olabileceği ve bu ağlarda dağılıma karşı alınabilecek önlemler irdelenmiştir.

*Anahtar Kelimeler: IPv6, Yeni Nesil Teknolojiler, Bilgisayar Ağları, IPv4, Güvenlik, Solucan*

## 1. GİRİŞ

20 yıldan fazla süredir ağ üzerinden cihazların bağlantısı için kullanılmakta olan Internet Protokolü (IPv4), bu süre zarfında hızla gelişen teknolojiye bağlı olarak beklentilerin çok üzerinde artan kullanıcı ihtiyaçlarını karşılamak konusunda yetersiz kalmıştır.

Yeni teknolojilerin getirdiği ihtiyaçların karşılanabilmesi için tasarlanmış olan yeni nesil internet protokolü IPv6; adres kapasitesi, dolaşılabilirlik, güvenlik, çoklu dağıtım, servis kalitesi ve yeni teknolojilere uyumluluk gibi IPv4'te sorun yaratan birçok konuya çözümü bünyesinde barındırmaktadır.

Yeni nesil IP protokolüne geçiş çalışmaları IPv4'ün giderek daha yetersiz kalması üzerine son yıllarda ivme kazanmıştır. IPv6 tüm dünyada İnternet'e bağlanmak için kullanılacak yeni standart olacaktır. Japonya'da kamu internet ağının 2007 yılı içinde, Amerika Birleşik Devletleri'nde ise tüm internet servis sağlayıcılarının 2008 yılı Ağustos ayında tamamen IPv6 destekler hale gelmesi hedeflenmektedir. Avrupa Birliği komisyonu 27 Mayıs 2008 tarihinde IPv6 kullanımı ve uyum için eylem planı açıklayarak 28 Mayıs 2008'i IPv6 günü ilan

etmiştir. Avrupa Birliği (AB) çerçeve programları kapsamında INIT, 6WINIT, 6NET, Euro6ix, 6Deploy gibi IPv6'ya geçiş ve yaygınlaştırma projelerine son beş yıl içinde 100 milyon Avro'dan fazla maddi destek vermiştir.

Dünyadaki bu gelişmelere paralel olarak IPv6 ağlarında solucan dağılımının nasıl olabileceğine dair çalışmalar başlamıştır. Solucanlar, yayılımlarında kullandıkları yöntemlerin bir sonucu olarak yüksek miktarda bant genişliği kullanmakta ve kısa zamanda ağa bağlı bir çok cihazı ele geçirebilmektedir. Bu durumun yarattığı etkiler internetin tüm iletişim altyapısını etkilemekte ve çok kısa bir zaman içinde tüm dünya çapına yayılan servis kesintilerine sebep olabilmektedir.

İnternette yayılan solucanların etkileri *Morris* (1998) solucanından itibaren hızlıca artmıştır. *Code Red* solucanı 19 Temmuz 2001 tarihindeki saldırısında bir gün içerisinde 359.000 bilgisayara bulaşmıştır [1]. Microsoft, bu solucanın aktif olduğu gün içerisinde yayılması muhtemel IIS sunucularının sayısını 6.000.000 olarak hesaplanmıştır [2]. *Code Red* solucanından sonra internet solucanları yeni bir aşamaya girmiş ve bunu *Code Red II*, *Nimda*, *Slammer*, *Blaster*, *Sasser* solucanları izlemiştir.

Makalenin ikinci bölümünde IPv6 protokolüne geçiş yöntemleri açıklanacak, daha sonra solucan dağılımının nasıl olduğu ve IPv6 ağlarında ne gibi değişikliklere uğrayacağı konusunda bilgiler verilecektir. Son olarak IPv6 solucanlarının konak aramak için hangi yöntemleri kullanabileceğine değinilecek ve yeni nesil IP protokolünün kullanıldığı ağlarda solucan dağılımı sebebiyle yaşanabilecek muhtemel sorunlar listelenecektir.

## 2. IPV6 PROTOKOLÜNE GEÇİŞ YÖNTEMLERİ

IPv4 ağlarının IPv6'nın yaygınlaşması ile birlikte zaman içinde sonlanacakları öngörülmektedir. Yeni bir protokole geçişte mevcut olan altyapının kullanılması bir anda bırakılamayacağından, bir süre iki protokolün internette aynı anda bulunması kaçınılmazdır. IPv6'ya geçiş için kullanılacak yöntemler şu şekilde gruplandırılabilir [3].

### 2.1. İkili yığın

Bu yöntemde cihazların iki protokolü de aynı anda desteklemesi söz konusudur.

### 2.2. Tünelleme

IPv6 ağlarının IPv4 ağları üzerinden diğer IPv6 ağlarına ulaşması için kullanılan yöntemdir. İstemciden istemciye, istemciden yönlendiriciye, yönlendiriciden istemciye, yönlendiriciden yönlendiriciye olmak üzere tünelin açılış şekline göre 4 grup altında toplanabilir.

### 2.3. Yalın IPv6

Sadece IPv6 adresine sahip olan ağ cihazlarının IPv4 cihazları ile konuşabilmeleri için çevirici (translator) kullanarak IPv6 <-> IPv4 çevriminin yapılmasıdır.

## 3. SOLUCAN DAĞILIMI

### 3.1. Solucan dağılımı aşamaları

Solucan yayılımı üç farklı aşama halinde incelenebilir:

#### 3.1.1. Sisteme sızmak için bir açık bulunması

Solucan dağılımının olabilmesi için solucanın ağ cihazına sızacak bir güvenlik açığı bulması gerekir. Solucanın yayılma hızı bulunan açığın yaygınlığı ile doğru orantılıdır. Yaygın olarak kullanılan servislerdeki açıkları kullanarak bulaşan bir solucan çok daha kolay yayılır.

#### 3.1.2. Bulunan açık yardımı ile konağa sızılması

Solucan bu aşamada konaktaki açığı kullanarak sisteme sızar ve sistem kaynaklarına erişim hakkı sağlar.

#### 3.1.3. Kendini kopyalama, başka konaklar arama

Solucan dağılımında en kritik aşama olan yeni sistemlerin bulunması ve bulaşılması aşamasıdır. Solucan yeni konakların tespit edilmesi için aşağıdaki yöntemlerin biri veya bir kaçını birlikte kullanabilir.

1. Tamamen rastgele IP taraması yapılması
2. İlk yayılma aşamasını hızlandırmak için açık olan sistemlerin rastgele tarama yöntemi ile tespit edilip solucana girdi olarak verilmesi
3. Bulaşılan sistemdeki yerel bilgilerin kullanılması (Elektronik posta ile bulaşan solucanın yeni hedef bulmak için adres defterini kullanması gibi)
4. Arama motorları benzeri dış kaynaklarla hedef arama.

Solucan yeni konak arama sürecini başarıyla tamamlar ise bir önceki bölümde anlatılan açık bulunması ve bu açıktan faydalanılması aşamalarını tekrarlar.

### 3.2. IPv6 ağlarında solucanların dağılmak için kullanabileceği yöntemler

IPv4'te olduğu gibi IPv6 ağlarında da solucanlar yeni konak bulmak için üzerinde koştukları konaktaki bilgileri ve dış kaynakları kullanacaklardır. Yeni hedef tespiti için konak üzerinde bulunan bilgilerin kullanılması IP nesline (IPv4, IPv6) bağlı olmayan bir durumdur. Bununla birlikte dış kaynaklar kullanarak yeni hedef arama metodları IPv6'nın gelmesi ile birlikte değişiklik gösterecektir. IPv4 tabanlı iletişim için geçerli olan yerel kaynakların kullanılması ve arama motorlarında sorgulama yapılması yöntemlerinden farklı olarak IPv6 solucanlarının kullanabilecekleri dış kaynaklar dört grupta toplanabilir.

#### 3.2.1. DNS kaba kuvvet (Brute Force)

Ağa bağlı cihazların IP adresleri yerine daha kolay tanımlanabilir ve hatırlanabilir bir isimlendirme sistemi olan DNS mekanizmasının kullanımı pratik bir uygulamadır. IPv4 tabanlı ağlarda DNS tanımlaması daha çok sunucular için yaygın bir yöntem olsa da IPv6 tabanlı ağlarda her bir adrese karşılık bir tanımın yapılması daha yaygın olarak uygulanmaktadır. Bunun nedeni, IPv6 adres kodlamasının 128 bit olması ve her bir IP adresinin 16 hegzadesimal karakterden oluşmasıdır. IPv6 ağlarında her bir IPv6 adresi için DNS kullanımı zorunluluğu, DNS sunucularına yapılacak olan bir kaba kuvvet saldırısı aracılığıyla ağda kullanılan IPv6 adreslerinin bulunması için uygun bir alan yaratmaktadır. Alan adı tanımı yapılırken kullanılan isimler genelde 6 karakterden az ve harf/sayı bileşiminden oluşmaktadır. 26 harf ve 10 rakam ile oluşturulabilecek 6 karakterlik dizilerin toplam sayısı

$36^6 = 2, 176,782,336$  adettir. Bu rakam IPv6 ile en az ağ aralığı olarak tanımlanabilecek olan /64 alt ağının içereceği  $2^{64}$  olasılıktan çok daha azdır. Bir kuruma ait alan adı altında bulunan tüm bilgisayarların IP adreslerine ulaşmak, DNS sözlük saldırısı ile desteklenmiş bir DNS kaba kuvvet saldırısı sonucunda mümkün olabilecektir. DNS kaba kuvvet saldırısı için yazılmış olan birçok uygulama vardır. TXdns [4] bu uygulamalara örnek olarak verilebilir. Yeni yazılacak olan solucanların bu yöntemi kullanarak kendilerine bulaşacak IPv6 ağ bileşeni aramaları mümkündür.

### 3.2.2. Ağ koklamak

IPv6 alt ağında ele geçirilen bir istemci diğer IPv6 adreslerini bulmak için ağ koklama yöntemine başvurabilir. IPv6 adresleri hakkında bilgi veren en önemli kaynaklardan biri IPv6 Adres Çakışması Belirlenmesi, DOD (Duplicate address detection), icmpv6 paketleri olabilir [5]. IPv6 adresi alacak olan bir bilgisayarın alacağı IPv6 adresini ağda olup olmadığını anlamak için gönderdiği IPv6 DOD paketleri koklanarak ağ adresleri öğrenilebilir. Diğer bir yöntem de IPv6'te DHCP protokolü işlevine göre IPv6 Yönlendirici "durum denetimsiz yapılandırma (stateless autoconfiguration)" anonslarının dinlenerek ağdaki cihazlar tarafından alınan IPv6 adreslerinin öğrenilmesidir.

### 3.2.3. Yönlendirici ele geçirmek

Saldırganlar tarafından ele geçirilen yönlendiricilerden akan trafikte kullanılan IPv6 adresleri öğrenilerek solucanlara hedef olarak verilebilir. Ağ cihazlarının üzerinden geçirdikleri trafik bilgilerini raporlama özelliği kullanılarak ağda IPv6 trafiği oluşturan cihazlara ait raporlar elde edilebilir. Bu raporların analizi sırasında belirli filtreler kullanılarak IPv6 kullanan sunucular belirlenebilir. Örneğin hedef olarak web sunucularının seçilmesi durumunda, 80 numaralı kapısına trafik giden IPv6 adresleri ayıklanarak hedefler belirlenebilir.

### 3.2.4. Rastgele IP adresi tarama

Rastgele IP adresi tarama yöntemlerinin temel dayanak noktası IP adres aralığının taranabilir sayıda olmasıdır. IPv4 ağlarında genelde kullanılan /24 adres aralığı 254 adet ağ cihazının adreslemesine izin verdiği için hızlı ağlarda saniyeler içinde yerel alan ağı taranabilmektedir. IPv6 yerel ağında önerilen adres uzunluğu /64 ve bu aralıkta adreslenebilecek ağ cihazı sayısı  $2^{64}$  olduğundan bu tür bir adres aralığının taranması seneleri bulmaktadır. Saniyede 1.000.000 adres taranması durumunda alt ağdaki tüm bilgisayarları bulmanızın 28.000 yıl alacaktır. Bu durum yerel alan ağı ve geniş alan ağındaki IPv6 adres aralığının

genişliğinin rastgele IP taraması yapan solucanların yayılmasının önüne geçeceği öngörüsünü içerse de IPv6 ve IPv4 adreslerinin beraber kullanıldığı ikili yığın yapısında çalışan ağlarda solucan yayılımının yalnız IPv4 çalışan ağlara göre daha hızlı olabileceğine dair araştırma sonuçları da mevcuttur [6]. Bununla birlikte DNS servisini alan adından IP adresine gitmek için kullanan solucanların mevcut olması durumunda solucan yayılma hızının IPv4 ağlarına yakın olduğuna dair araştırmalar bulunmaktadır [7].

## 3.3. IPv6'nın solucan dağılımına etkileri

### 3.3.1. IPv6'nın yeni bir protokol olması

IPv6 protokolünün getirdiği yeni nesil özellikler solucanların yayılmasını kolaylaştırabilir. IPv4'ün uzunca süredir kullanılması ağ cihazlarının üzerindeki yazılımları güvenlik açısından kararlı hale getirmiştir. Bununla birlikte ağ cihazlarının IPv6 uyumlu hale getirilmesi sırasında yeni açıklar doğabilmektedir. Felsefi güvenli kod yazmak olan OpenBSD işletim isteminde 10 senede çıkan ikinci açığın IPv6 kaynaklı olması düşündürücüdür. Benzer şekilde yaygın olarak kullanılan Windows işletim sistemlerinde IPv6 ile ilgili servis dışı bırakma saldırılarına imkan veren açıklar bulunmaktadır.[8] Linux işletim sisteminde de IPv6 Jumbo paketlerini kullanarak servis dışı bırakma açığı bulunmaktadır. [9] Buna benzer açıkların IPv6'ya geçiş aşamalarında ortaya çıkması, bu açıkları kullanılarak yayılan IPv6 solucanların yazılması olasılığını arttırmaktadır.

### 3.3.2. IPv6 geçiş aşamasında yaşanabilecek problemler

IPv4 ve IPv6 ile uyumlu düğümlerin bulunduğu ikili yığın ağlarda solucan dağılımının daha hızlı olabileceği görüşünü savunan çalışmalar yürütülmüştür [6,10].

### 3.3.3. Yeni cihazların ağa katılması

İletişiminin IP tabanlı teknolojilere doğru gitmesi, IPv6 kullanan solucanların bulaşacak konak çeşitliliğinin artacağı anlamına gelmektedir. Kablosuz teknolojilerin yaygınlaşması ile birlikte her türlü cihazın ağa bağlanması solucan sorununun bilgisayardan çıkıp IP konuşan cep telefonu, PDA ve benzeri cihazlara bulaşmasını sağlayacaktır. Bu durumun getireceği problemler aşağıdaki şekilde özetlenebilir:

- Günümüzde güvenlik araçları bilgisayar üzerine koşacak şekilde yazılmıştır. IP konuşabilen cihazlarda da, bilgisayarda olduğu gibi koruma yazılımları (anti-virüs, anti-spam

- vb ) geliştirilip konuşlandırılması gerekecektir.
- IP konuşan cihazların işletim sistemlerinin gömülü olması durumunda güncelleme yapmak daha da zor olacaktır.
- IP konuşan cihazlarda bilinen açıkların var olup olmadığını anlamaya yarayacak veya çıkarılan yamaları işletim sistemine uygulamaya yetecek kadar bellek ve işlemci gücü olmayabilir.

### 3.3.4. IPv6 ağlarının izlenmesi

İnternette solucan yayılımının önüne geçmenin en verimli yolu solucan dağılımını başlangıç seviyesinde yakalayarak gerekli olan tedbirleri almaktır [11].

Cliff C. Zou, Weibo Gong, Don Towsley ve Lixin Gao tarafından yapılan araştırmada internet solucanlarının yayılımlarının erken aşamalarında farkına varmak için önerilen sistemde, yayılımın saptanabilmesi için sensör sayısının fazlalığının ve çeşitliliğinin önemi vurgulanmaktadır.[11] Bu sebeplerden dolayı IPv6 ağlarında cihazların aktivitelerinin izlenmesinin önemi artacaktır.

## 4. IPV6 AĞLARINDA SOLUCAN DAĞILIMINA KARŞI ALINABİLECEK ÖNLEMLER

Yeni solucanların dağılımlarının erken aşamalarında farkına varıp gerekli tedbirlerin alınabilmesi için IPv6 ağlarına balküpu (honeypot) uygulamaları konuşlandırılmalıdır.

IP konuşan cihazların yazılım güncellemeleri ve yama mekanizmaları otomatik hale getirilmelidir.

Ağda alınacak önlemlerin IPv6 konuşan cihazların çeşitliliği nedeni ile uç noktada alınmasının güçlüğü, güvenlik önlemlerinin bir kısmının IPv6 bağlantısını saplayan ağ cihazlarında alınması ile aşılabılır. Örneğin DHCP saldırılarının önüne geçmek için anahtarlama cihazlarında kullanılan ve sadece izin verilen kapılardan DHCP isteklerine cevap verilmesine olanak sağlayan önlemin benzeri alınabilir. IPv6 durum denetimsiz (stateless) yapılandırma paketlerine, sadece yönlendiricinin bağlı olduğu kapıdan cevap verilmesi şeklinde özetlenebilecek bu önlem ilgili yeteneğin anahtarlama cihazlarına kazandırılarak yalnızca yetkili olan sunucunun cevap vermesine yol açacaktır.

## 5. SONUÇ

Elektronik ticaretin bilgisayar dışında telefonla ve diğer mobil cihazlarla yapılması ekonomik açıdan da mobil ortamda yayılacak IPv6 solucanının vereceği zararın boyutunu arttıracaktır.

Elektronik ticaretin IPv6 konuşan cihazlardan yapılması zararlı kod yazan kişilerin ilgisini bu tip cihazlardaki açıkları arama ve kullanmaya itecektir.

Yeni solucanların yakalanmasında imza tabanlı çözümler yetersiz kalacağından davranışsal (Behavioral ) tabanlı yöntemlerin kullanımı artacaktır.

Geçiş aşamasında IPv4 ve IPv6'nın beraber kullanılması durumunda iki protokolün beraber yönetilmesi ile birlikte ortaya çıkabilecek olan karmaşıklıktan yeni açıklar doğacaktır.

IPv6 solucan yayılımı sırasında DNS sunucularının IPv6 adreslerine ulaşmak için kullanılması olasılığı yüksek olduğundan DNS sunucuları servis dışı kalabilecektir. Bu tür durumlara karşı önlemler alınmalıdır. Benzer şekilde solucanlar tarafından bilgi almak için kullanılacak olan IPv6 "herhangi birine gönderim" (anycast) adresleri üzerinden servis veren ağ cihazları da solucan dağılımı sırasında servis dışı kalabileceklerdir.

Yayılmak için adres kayıt defteri, arama motorları gibi kaynakları kullanan solucanların davranışları ve yayılmaları IPv6 ağlarında bir değişiklik göstermeyecektir.

## 6. KAYNAKÇA

- [1] [online] CAIDA, the Cooperative Association for Internet Data Analysis  
[http://www.caida.org/research/security/code\\_ed/coderedy\\_2\\_analysis.xml](http://www.caida.org/research/security/code_ed/coderedy_2_analysis.xml)
- [2] C.C. Zou, W. Gong, and D. Towsley. Code Red Worm Propagation Modeling and Analysis. In *9th ACM Symposium on Computer and Communication Security*, pages 138-147, Washington DC, 2002.
- [3] 6Net IP Deployment Guide  
<http://www.6net.org/book/deployment-guide.pdf>
- [4] <http://www.txdns.net/>
- [5] Qinhua Zheng , Ting Liu , Xiaohong Guan , Yu Qu , Na Wang " A New Worm Exploiting IPv4-IPv6 Dual-stack Networks " *Proceedings of the 2007 ACM workshop on Recurring malware* Sayfa 9-15

- [6] Zheng, Q., Liu, T., Guan, X., Qu, Y. & Wang, N. (2007). A new worm exploiting IPv4-IPv6 dual-stack networks. *Proceedings of the 2007 ACM workshop on Recurring malware*, 9-15.
- [7] Kamra, A., Feng, H., Misra, V. & Keromytis, A. (2005). The Effect of DNS Delays on Worm Propagation in an IPV6 Internet. *Proceedings of IEEE Infocom*, Miami, USA
- [8] [online] Vulnerabilities in TCP/IP IPv6 Could Allow Denial of Service (922819)  
<http://www.microsoft.com/technet/security/Bulletin/MS06-064.mspx>
- [9] [online] Linux Kernel IPv6 Jumbo Bug  
<http://www.securiteam.com/exploits/5QPOF15N5Q.html>
- [10] Keromytis, A.D., Bellovin, S.M. & Cheswick, B. (2006). Worm Propagation Strategies in an IPv6 Internet, *USENIX*, 31(1), 70 – 76
- [11] Cliff C. Zou, Weibo Gong, Don Towsley, Lixin Gao Pages “The monitoring and early detection of Internet worms” *IEEE/ACM TRANSACTIONS ON NETWORKING*, VOL. 13, NO. 5, Ekim 2005 Sayfa 961 - 974