DNS Güçlendirme Saldırısı Risk Analizi

Devrim Seral

***Özet*—Son zamanlarda meydana gelen çok büyük Dağıtık Servis Engelleme Saldırılarının ardında DNS güçlendirme saldırılarının tetikçi olduğu bilinmektedir. Bu saldırı türü, dağıtık servis engelleme saldırılarını, farklı ağlardaki özyinelemeye açık DNS sunucuları aracı olarak kullanarak yerine getirmektedir. Bu sistemlerin tespit edilerek tanımlanmaları uzun ve zahmetli bir işlemdir. Bu yüzden bu çalışmada, çalışma kümesi olarak Kuzey Kıbrıs Türk Cumhuriyetinde faaliyet gösteren biri kamu olmak üzere toplamda sekiz adet İnternet Servis Sağlayıcı ağı kullanılmıştır. Geliştirilen bir betikle bu ağlar üzerinde tespit edilen özyinelemeye açık DNS sunucuları ile ilgili toplanan bilgiler sunulmuş ve yaratabilecekleri riskler ortaya konmuştur.**

Anahtar Kelimeler—DDoS, DNS, DNS Güçlendirme Saldırısı

***Abstract*— DNS amplification attacks are known as perpetrator of today's very huge Distributed Denial of Service attacks. This type of attack performs distributed denial of service attack through open recursive DNS servers located in different locations. Discovering and identifying open recursive DNS servers are time consuming and troublesome process. Therefore in this study we use eight Internet Service Provider (One of them government internet provider) networks that operate at Turkish Republic of Northern Cyprus as a working set. A script developed to identifying and collecting information for open recursive DNS servers that available in these networks and risks that sourced by these systems expressed.**

Index Terms—DDoS, DNS, DNS Amplification Attack

I. GİRİŞ

İNTERNET kullanımının sürekli olarak artması ile birlikte servis veren kurum ve şirketlerin erişilebilir olması, gittikçe daha da önemli bir hale gelmiştir. Türkiye'de 2013 yılı ilk üç aylık dönemde geniş bant İnternet abonesi sayısı 20 milyon kişiyi aşmış ve bu abonelerin %78 gibi büyük bir kısmının 8Mbps hıza kadar bağlantı sunan paketleri tercih ettikleri görülmüştür [1]. Ayni zamanda Bankalararası Kart Merkezi verilerine göre 2013 yılı sonuna kadar İnternet üzerinden harcanması beklenen para miktarı 34 milyar TL'ye ve yapılan işlem miktarının da 160 milyonu bulması beklenmektedir [2]. Dünyanın diğer ülkelerinde de ITU (International Telecommunication Union) verilerine göre 2.7 milyar kişinin geniş bant İnternet bağlantısına sahip olduğu bilinmektedir [3]. Diğer yandan 2013 yılı içinde e-ticaretin 1.3 trilyon dolarlık bir büyüklüğe ulaşacağı tahmin edilmektedir [4]. Bu bilgiler ışığında dünyanın birçok ülkesinde gerek kamu gerekse özel şirketlerin çevrimiçi hizmet sayısını sürekli artırdığı kuşku götürmez bir gerçektir. Bu kadar fazla ekonomik büyüklüğe ve kullanıcı sayısına ulaşan çevrimiçi servislere rekabetten, pazar paylaşımından ve hatta siyasi yada politik nedenlerle sorun çıkarmak isteyenlerin bulunması kaçınılmaz olmaktadır. İnternet üzerinden verilen servislere erişimi engellemek için kullanılan en yaygın yöntemlerden biri Hizmet Engelleme Saldırılarıdır (Denial of Service). Bu türdeki saldırılarda, saldırgan hizmeti veren sistemin ağ kaynaklarını yada diğer kaynaklarını (hafıza, işlemci, disk vs.) tüketerek gerçek sistem kullanıcılarının İnternet servislerine erişimini engellemektedir [5]. Hizmet Engelleme Saldırılarının günümüzde en yaygın olanı Dağıtık Hizmet Engelleme Saldırılarıdır (Distributed Denial of Service). Dağıtık Hizmet Engelleme Saldırıları özellikle özel şirketlere saatte 10,000$'dan başlayan miktarlarda mali kayıplara neden olabilmektedir [6]. Bu tür saldırılar kurumlara mali kayıpların yanında ayrıca prestij kaybına da yol açmaktadır. Bu saldırıların ne tür sistemlerden kaynaklandığını bilmek, saldırıları önlemek yada engellenebilmesine yardımcı olmaktadır. Örneğin, Cloudflare şirketinin bir müşterisine, 2012 yılının Eylül ayında 65 Gbps büyüklüğe ulaşan ve Dağıtık Hizmet Engelleme Saldırısının bir türü olan DNS Güçlendirme (Domain Name System Amplification) saldırısı olduğu firma tarafından tespit edilmiştir [7]. DNS Güçlendirme saldırıları ile ilgili önemli bir uyarıda Mart 2013'de Amerika Birleşik Devletleri CERT'den (Computer Emergency Readiness Team) gelmiştir [8]. Bu çalışmanın temel amacı İnternet servislerinde ciddi kesintiye yol açabilecek DNS Güçlendirme saldırısı hakkında bilgi sunarak, bu saldırının tetikçi olarak kullandığı özyinelemeye açık ağ alan çözümleme sistemleri ile ilgili çalışma kümesi olarak kullanılan sekiz adet İnternet Servis Sağlayıcı ağından elde edilen bulgular paylaşılacaktır. Makalenin bundan sonraki bölümleri şu şekildedir; 2. Bölümde DNS Güçlendirme saldırısının çalışma yöntemi ele alınacak, 3. Bölümde bu saldırı türünün aracı olarak kullandığı açık alan adı çözücüleri tespit etmek için geliştirilen betik ve çalışma kümesi anlatılacak, 4. Bölümde elde edilen veriler paylaşılarak ve son olarak Sonuç kısmında bu bulgular değerlendirilecektir.

II. DNS GÜÇLENDİRME SALDIRISI

Bu bölümde önce DNS sisteminin çalışması ile ilgili genel bilgi verilecek daha sonra DNS Güçlendirme saldırısının çalışma yöntemi anlatılacaktır.

A. DNS Nedir?

DNS İnternetin çalışmasını sağlayan gizli kahramanlardan biridir. DNS sisteminin temel görevi istemcilerden gelen alan adı yada sistem isimlerini bilgisayarların anlayacağı adreslere çevirmektir [9]. Ayni zamanda gelen adres bilgilerini isimlere de çevirebilir. Bu sistemler istemci sunucu mimarisinde çalışır ve istek ve cevap bilgisini UDP

Devrim Seral, Uluslararası Kıbrıs Üniversitesi, Mühendislik Fakültesi, Bilişim Sistemleri Mühendisliği, Lefkoşa-Kıbrıs'ta öğretim üyesidir. (e-mail: dseral@ciu.edu.tr)

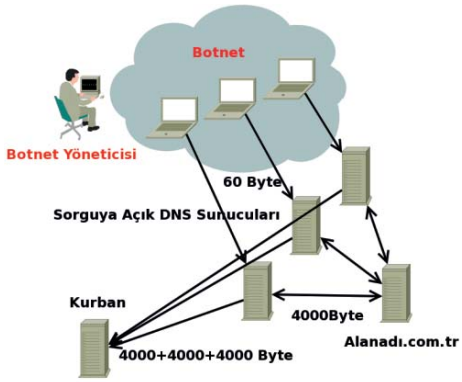
(User Datagram Protocol) protokolü kullanarak taşır.

DNS sistemlerinin 1980'li yıllardan itibaren kullanılmaya başlanmasından sonra sürekli olarak yenilenmiş ve bu alanda ilk uygulama BSD sistemleri üzerinde geliştirilen BIND yazılımı olmuştur [10].

B. *DNS Güçlendirme Saldırısı Nedir?*

İnternet kullanıcı sayısı ve trafiğinin 1990'lı yıllarda artmaya başlaması ile birlikte DNS sistemleri gittikçe önem kazanmıştır. Bundan dolayı DNS sistemlerinin çalışma doğasından gelen açıklar çıkmaya başlamıştır. 2004 yılında Atkins ve Austein RFC 3833 belgesinde DNS sisteminin zayıflıklarının analizini yapmışlardır [11]. Bu belgenin Hizmet Engelleme Saldırıları kısmında DNS Güçlendirme saldırısının yapılabileceğine dair bilgi vermişlerdir. 2006 yılında yapılan diğer bir çalışmada DNS Güçlendirme saldırısının nasıl yapılabileceği ile ilgili ayrıntılı bilgi verilmiştir [12].

DNS Güçlendirme Saldırısı ilke olarak Smurf saldırısının bir benzerini ICMP isteği yerine DNS istek paketleri kullanarak yerine getirmektedir [13]. DNS Güçlendirme Saldırısının nasıl yapıldığını bir senaryo ile anlatmak daha kolay olacaktır. Şekil 1'de DNS Güçlendirme Saldırı senaryosunda gösterildiği gibi, saldırganın Botnet [14] üzerinden binlerce bilgisayarı kontrol ettiğini, Botnet'e dahil olan cihazların kaynak adreslerini kurbanın adresi olarak değiştirerek binlerce DNS sorgusunu, dışarı özyineli sorgulamaya açık DNS sunucularına gönderdiğini varsayalım. Böyle bir saldırıda her bir DNS isteğinin 60 Byte'lık paket boyutunda gönderilebileceğini varsayarsak sorgulama yapılan sunucular eğer EDNS [15] formatında ise cevabın boyutu 4000 Byte'ı aşabilir. Bu sayede 60 Byte'lık bir istek 60 kat güçlenerek kurbanın adresine geri dönebilir. Böylece Botnet üzerindeki saldırıya dahil olan her bir makinenin ürettiği isteğin 60 katı kadar trafik kurbanın üzerine yönlendirilebilmektedir [16].



Şekil 1. DNS Güçlendirme Saldırı senaryosu.

C. *DNS Güçlendirme Saldırısı Nasıl Engellenebilir?*

DNS Güçlendirme Saldırıları aşağıda verilen yöntemlerle engellenebilir [12]:

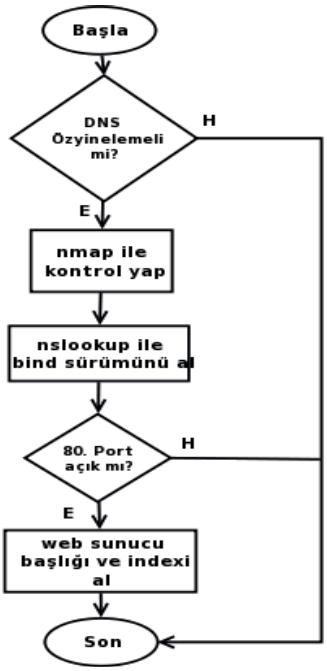
- Özyineleme yapan DNS sunucuların sadece hizmet verilen istemci IP bloklarına cevap verecek şekilde yapılandırılması.
- DNS sunucular eğer özyineleme işlemini tüm istemcilere açık tutmak zorundaysa, bir istemciden gelen istek sayısı belirli oranın üzerinde olması durumda o istemciye cevap vermeyi kesebilir.
- İstemcilere İnternet erişimi veren servis sağlayıcıların IP hilekarlığını (spoofing) önleyici yöntemler uygulaması.

III. ÖZYİNELEMEYE AÇIK DNS SUNUCU TESPİTİ

Bu bölümde özyinelemeye açık DNS sunucuları tespit etmek için geliştirilen betik ve çalışma kümesi ele alınacaktır.

A. *Yöntem*

DNS Güçlendirme Saldırılarına olanak veren en temel neden özyinelemeye açık DNS sunucularıdır. İnternet üzerindeki herhangi Botnet ağından, yanlış yapılandırma yada başka nedenlerle sorgu yapan tüm cihazlara özyinelemeli olarak cevap veren bu türdeki DNS sunucuları doğrudan bu Dağıtık Servis Engelleme Saldırısına yardımcı olmaktadır. Bu yüzden Şekil 2'de akış şeması verilen bir betik yardımı ile bu türde saldırılara olanak veren sunucular bazı özelliklerine göre tespit edilmişlerdir.



Şekil 2. Özyinelemeye açık DNS sunucuları tespit eden betiğin akış şeması..

Özyinelemeye açık DNS sunucuları tespit eden betiğin çalışma adımları aşağıdaki gibidir.

a) Betik, hedef olarak verilen sistemin DNS sorgu portuna (UDP/53) kendi kontrolünde olması mümkün olmayan bir alan adı için (Ör: isc.org) DNS istemcisi ile sorgu gönderir. Eğer hedef sistem DNS sorgularına özyinelemeli olarak cevap veriyorsa bu sistem saldırı için uygun olarak işaretlenir. Cevap vermiyorsa betik diğer sistemleri kontrole devam eder.

b) Özyinelemeli olarak cevap alınan hedef sistemin diğer karakteristiklerini tespit etmek için nmap [17]

port tarama uygulaması ile bazı önemli portları taranarak alınan sonuçlar kaydedilir.

c) DNS sorgulama araçları ile CHAOS sınıfı kullanılarak eğer mümkünse DNS sunucunun sürümü tespit edilir [18].

d) Yine hedef sunucunun HTTP (Hyper Text Transfer Protocol) portu açıksa web sunucunun türü tespit edilir.

B. *Betik Çalışma Kümesi*

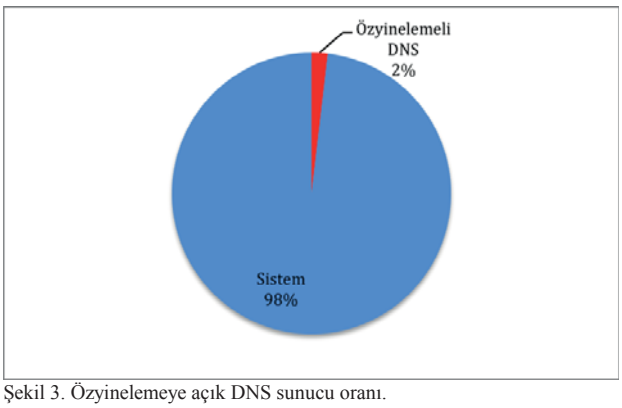
Özyinelemeye açık DNS sunucuları tespit etmek zahmetli ve uzun süren bir işlem olmasından dolayı, betiğin çalışma kümesi olarak Kuzey Kıbrıs Türk Cumhuriyeti sınırları içinde faaliyet gösteren biri kamu olmak üzere sekiz adet İnternet Servis Sağlayıcı (İSS) ağı kullanılmıştır. Çalışmanın yapıldığı bu ağlar mobil İnternet haberleşme dışındaki yaklaşık olarak tüm geniş bant İnternet abonelerini kapsamaktadır. Toplamda test edilen IP adresi sayısı 28416 adet olmuştur. Betik çalışması kontrollü bir şekilde yapılarak test yapılan ağların bu işlemi saldırı yada keşif olarak algılamaması sağlanmaya çalışılmıştır.

IV. ÖZYİNELEMEYE AÇIK DNS SUNUCU BULGULARI

Geliştirilen betik ile toplanan veriler bu bölümde verilecektir.

A. *Özyinelemeye Açık DNS Sunucusu Oranları*

Bölüm III'de ayrıntısı verilen betik ile yapılan analizler sonrası toplamda 28416 IP'den oluşan ve değişik boyutlarda ağlar içeren sekiz ağda bulunan sistemlerden sadece 542'si yada %2'si Özyinelemeye açık DNS sunucu olarak çalışmaktadır. Bu oran Şekil 3'de gösterilmiştir.



Şekil 3. Özyinelemeye açık DNS sunucu oranı.

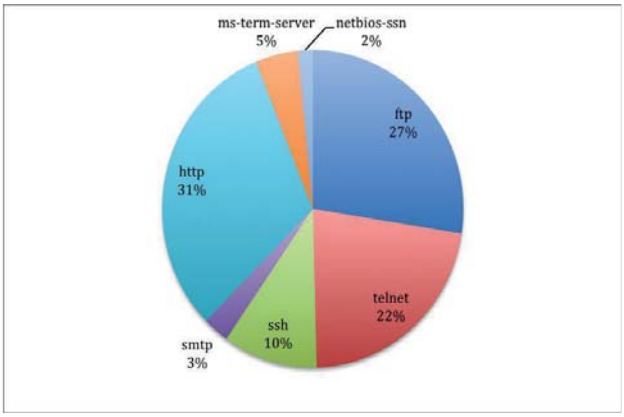
B. *Özyinelemeye Açık Sistemler Üzerindeki Diğer Açık Portlar*

542 adet makine üzerinde DNS dışında çalışan diğer servisleri de tespit edebilmek üzere nmap [17] port tarama uygulaması ile en fazla kullanılan TCP portlarından 21'den 25'e kadar, 80, 139 ve 3389 portları üzerinde tarama yapılmıştır. Ayni zamanda 111 ve 137 UDP portları da taranmasına rağmen UDP protokolünün doğası gereği bu portların durumu hakkında tam anlamıyla doğru bir bilgi alınamamıştır. Tablo I'de nmap ile test edilen ve açık olduğu tespit edilen TCP portların sayıları gösterilmektedir.

TABLO I
AÇIK PORT SAYILARI

Port	ftp	telnet	ssh	smtp	http	Ms-term server	Netbios
Sayı	138	111	51	14	157	23	8

Yine Şekil 4'de açık olan portların diğerlerine göre yüzdelik dağlımı verilmiştir. Bu bilgiler ışığında Özyinelemeye açık DNS sunucu içeren bu sistemlerde UDP 53 dışında ayrıca http ve ftp daha sonra telnet portunun açık olduğu tespit edilmiştir. http,telnet ve ssh portları bu sistemlerin uzaktan yönetilebilir yada yönetilmeye müsait olduklarını göstermektedir. FTP portunun açık olması da bu sistemlerin sadece basit uzaktan yönetilebilir sistemler olmadıklarını bunun yanında kurulum bilgilerinin ya da değiştirilebilir web sayfaları gibi hizmetler de verebildiklerini göstermektedir.



Şekil 4. Sistemler üzerinde açık olan portlar.

C. *HTTP Portu Açık Sistemlerde Çalışan Web Sunucu Türleri*

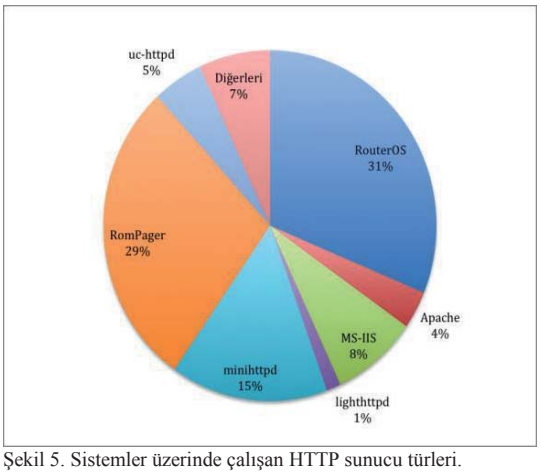
HTTP portu (TCP/80) açık olan sistemler üzerinde HTTP isteğine verilen cevap başlığı üzerinde yapılan analiz sonucu tespit edilen web sunucu türleri Tablo II'de verilmiştir.

TABLO II
WEB SUNUCU TÜRLERİ

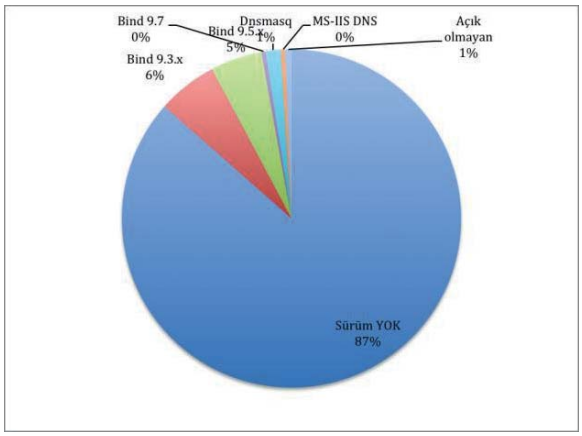
Türü	Rom Pager	Mini httpd	MS-IIS	Uc httpd	Apache	Router OS	Light httpd	Diğer
Sayı	41	22	12	7	5	45	2	10

Şekil 5'de Web sunucu türlerinin yüzdeleri gösterilmektedir.

HTTP geri dönüş başlık bilgisinden sadece 99 sistemin web sunucu türü öğrenilebilmiştir. Ancak istek sonucu cevap olarak gelen sayfa verileri üzerinde yapılan analizle 45 adet sistemin de Mikrotik RouterOS işletim sistemi üzerinde çalıştığı tespit edilmiştir. Burada dikkat çekici olan Web sunucu türleri RomPager, Mini-httpd ve RouterOS şeklinde sıralanmaktadır. Kendini RomPager yada mini-httpd olarak tanıtan sistemler üzerine rastgele web istemci ile bağlantı yapıldığında bu cihazların ADSL modem cihazları yada gömülü sistemler olduğu görülmüştür. RouterOS ise genelde kablosuz sistemlerde kullanılan özel gömülü sistemlerin işletim sistemidir.



Şekil 5. Sistemler üzerinde çalışan HTTP sunucu türleri.



Şekil 6. Sistemler üzerinde çalışan DNS sürümlerinin oranları.

D. DNS sürümü kontrolü

DNS sorgulama araçları ile CHAOS sınıfı kullanarak DNS portu (UDP/53) açık olan cihazların sürüm bilgisi betik ile sorgulanmıştır. Tablo III'de tespit edilebilen sunucu türleri gösterilmektedir. Tespit edilen sunucu türlerine göre bu cihazların %12'si Unix yada türevi cihazlar ve ISC Bind sürümünü çalıştırdığı görülmektedir. İki adet sunucu ise Microsoft firmasının IIS DNS sunucusunu çalıştırmaktadır. Dns-masq sunucular ise DNS sorgularını yönlendirerek yapan genelde güvenlik duvarı sistemleri üzerinde kullanılan sistemlerdir. Geriye kalan %87 DNS sunucuları ise, Bind dışında muhtemelen özel olarak gömülü sistemler için tasarlanmış bir DNS sunucusu çalıştırmaktadır.

TABLO III
DNS SUNUCU TÜRLERİ

Sunucu	Bind 9.3.x	Bind 9.5.x	Bind 9.7	Dns masq	MS-IIS	Sürüm Yok
Sayı	28	24	2	7	2	424

Şekil 6'da Özyinelemeye açık DNS sunucuların tespit edilen DNS sürümlerinin yüzdeleri gösterilmektedir.

V. SONUÇ

Bu çalışmada KKTC'de faaliyet gösteren biri kamu toplamda sekiz adet büyük İnternet Servis Sağlayıcı ağına dahil olan, 28416 IP numarası üzerinde Dağıtık DNS Güçlendirme Saldırısına yardımcı olabilecek Özyinelemeli DNS çağrısına açık DNS sunucuları tespit edilmiştir. Tespit edilen özyinelemeye açık DNS sunucuları her ne kadar da bütün içinde %2'lik bir oranda olsa da, bu cihazların her biri üzerinden belirlenmiş bir kurbana doğru 1 Mbps saldırı yapılabilirse, kurban üzerinde yaklaşık 500 Mbps'lik bir Dağıtık Servis Engelleme Saldırısı gerçekleştirilebilir. Bu büyüklükte gerçekleştirilebilecek bir saldırı coğrafyamızda çoğu şirket ve kurumun baş edemeyeceği bir trafik miktarını ifade etmektedir. Diğer yandan özyinelemeye açık DNS sistemlerinin, ne tür cihazlar oldukları geliştirilen bir betik ile tespit edilmeye çalışılmıştır. Çalışmanın dördüncü bölümünde ayrıntıları da verildiği üzere özyinelemeye açık DNS sunucuların çok büyük bir kısmı ön tanımlı olarak dışarı doğru DNS çağrısına izin veren gömülü sistemlerdir. Bunların dışında kalan DNS sunucuları ise operatörler tarafından yanlış olarak yada gereksinimden dolayı yapılandırılmış sunuculardır. Bu saldırı türünün başarılı olmaması için alınacak birinci önlem, operatörlerin kendi ağ adreslerini taşımayan ancak kendi ağlarından kaynaklanan ağ trafiklerini engellemeleri, ikincisi ise operatörler tarafından son kullanıcılara satılan yada verilen cihazların yapılandırma yapılırken yerel ağ dışında DNS sorgularına cevap vermesinin engellenmesi ile olacaktır.

TEŞEKKÜR

Bu çalışmada sistemlerini ve İnternet bağlantısını kullanmama izin veren sayın Mehmet Alptürk'e teşekkür ederim.

KAYNAKLAR

[1] Sektörel Araştırma ve Strateji Geliştirme Başkanlığı. (2013, Mart). Üç Aylık Pazar Verileri Raporu [Çevrimiçi]. Bağlantı adresi: http://www.tk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/ucaylik13_1.pdf

[2] Bankalararası Kart Merkezi. (2013,Haziran). Haziran 2013 Aylık Bülteni [Çevrimiçi]. Bağlantı adresi: http://www.bkm.com.tr/basin/bultenler/aylik_bulten_052013.pdf

[3] ITU (2013). ICT Fact Figures 2013 [Çevrimiçi]. Bağlantı adresi: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf

[4] T. Fredriksson (2013,Nisan). E-commerce and Development Key Trends and Issues [Sunum]. Bağlantı adresi: http://www.wto.org/english/tratop_e/devel_e/wkshop_apr13_e/fredriksson_ecommerce_e.pdf

[5] CMU-CERT (1997,Ekim). Denial Of Service Attacks [Çevrimiçi]. Bağlantı adresi: http://www.cert.org/tech_tips/denial_of_service.html

[6] Neustar (2013,Nisan). 2012 Annual DDOS Attack and Impact Survey: A Year-to-Year Analysis [Çevrimiçi]. Bağlantı adresi: http://www.neustar.biz/enterprise/docs/whitepapers/ddos-protection/2012-ddos-attacks-report.pdf

[7] M. Prince (2012,Eylül). How to lunch a 65Gbps DDoS, and How to Stop One [Çevrimiçi]. Bağlantı adresi: http://blog.cloudflare.com/65gbps-ddos-no-problem

[8] US-CERT (2013,Mart). Alert (TA13-088A) DNS Amplification attacks [Çevrimiçi]. Bağlantı adresi: http://www.us-cert.gov/ncas/alerts/TA13-088A

[9] P. Mockapetris (1983, Kasım). Domain Names – Concepts and Facilities [Çevrimiçi]. Bağlantı adresi: http://tools.ietf.org/html/rfc882

[10] Douglas Brian Terry, Mark Painter, David W. Riggle and Songnian Zhou, The Berkeley Internet Name Domain Server, Proceedings USENIX Summer Conference, Salt Lake City, Utah, Haziran1984, Sayfa 23-31.

[11] D. Atkins, R. Austein (2004, Ağustos). Threat Analysis of the Domain Name System (DNS) [Çevrimiçi]. Bağlantı adresi: http://tools.ietf.org/html/rfc3833

[12] R. Vaughn, G. Evron (2006). "DNS amplification attacks,". [Çevrimiçi]. Bağlantı adresi: http://www.isotf.org/news/DNS-Amplification-Attacks.pdf
[13] CMU-CERT (1998,Ocak). Alert (CA-1998-01) Smurf IP Denial-of-Service Attacks [Çevrimiçi]. Bağlantı adresi: http://www.cert.org/advisories/CA-1998-01.html
[14] B. McCarty, "Botnets: big and bigger", Security & Privacy, IEEE (Volume:1 , Issue: 4), s. 87-90, Haziran-Ağustos 2003.
[15] P. Vixie, (1999,Ağustos). "Extension mechanisms for DNS (EDNS0)," RFC-2671. [Çevrimiçi]. Bağlantı adresi: http://www.ietf.org/rfc/rfc2671.txt
[16] S. Changhua, L. Bin, S. Lei, "Efficient and low-cost hardware defense against DNS amplification attacks," in Proc. IEEE Global Telecommunications Conf. (GLOBECOM'08), Aralık 2008, pp. 1-5.
[17] G. F. Lyon. "Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning" Insecure, 2009.
[18] S.Woolf, D. Conrad (2007, Haziran). Requirements for Mechanism Identifying a Name Server Instance [Çevrimiçi]. Bağlantı adresi: http://tools.ietf.org/html/rfc4892

Devrim Seral 1977 yılında Kıbrıs'ın Lefkoşa şehrinde doğdu. Lisans eğitimini Ankara'da bulunan Gazi Üniversitesi Teknik Eğitim Fakültesinde 1998 yılında tamamladıktan sonra ayni üniversitenin Fen Bilimleri Enstitüsünden 2000 yılında Master ve 2007 yılında Doktor unvanlarını alarak mezun oldu. Doktora eğitimini sürdürdüğü sırada aynı zamanda özel sektörde bilişim alanında Sistem Mühendisi ve İnternet Mühendisi olarak çalıştı. 2007 Şubat ayında Uluslararası Kıbrıs Üniversitesi Mühendislik Fakültesinde öğretim görevlisi olarak akademisyenlik hayatına geri döndü. Şu anda ayni üniversitenin Bilişim Sistemleri Mühendisliği bölüm başkanlığını sürdürmektedir.

Dr. Seral, İşletim Sistemleri, Yük Dengeleme, Ağ güvenliği gibi konularda çalışmakta ve ayni zamanda Association for Computing Machinery ve IEEE üyesidir.