Süleyman Demirel Üniversitesi
Fen Bilimleri Enstitüsü Dergisi
Cilt 23, Sayı 1, 238-244, 2019

Süleyman Demirel University
Journal of Natural and Applied Sciences
Volume 23, Issue 1, 238-244, 2019

DOI: 10.19113/sdufenbed.507948

Siber Terör ve DDoS

Süreyya ATASEVER*[1], İlker ÖZÇELİK[2], Şeref SAĞIROĞLU[3]

[1]Gazi Üniversitesi, Bilişim Enstitüsü, Bilgisayar Bilimleri Bölümü, Ankara
(ORCID: https://orcid.org/0000-0002-6615-1472)
[2]Recep Tayyip Erdoğan Üniversitesi, Mühendislik Fakültesi, Elektrik-Elektronik Mühendisliği Bölümü, Rize
(ORCID: https://orcid.org/0000-0002-2032-1640)
[3] Gazi Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Ankara
(ORCID: https://orcid.org/0000-0003-0805-5818)

(Alınış / Received: 04.01.2019, Kabul / Accepted: 31.03.2019, Online Yayınlanma / Published Online: 26.04.2019)

Anahtar Kelimeler
DDoS,
Siber terör,
DDoS saldırı sınıfları,
DDoS saldırı motivasyon

Özet: Siber terörizm eylemlerinde etkili bir araç olarak kullanılan DDoS saldırıları 1980'li yıllarda amatör bilgisayar korsanları (script kiddies) tarafından oyun/gösteriş amaçlı gerçekleştirilmeye başlamıştır. Bu saldırılar ile ciddi ekonomik zararlar verebileceğini fark eden siber suçlular, 90'lı yıllarda DDoS saldırılarını elektronik ticaret şirketlerinden şantaj ile para kazanma aracı olarak kullanmaya başlamışlardır. 2000'li yıllarda ise DDoS siber protesto ve saldırı aracı olarak kullanılmaktadır. Bu çalışmada DDoS saldırılarının gerçekleştirilme nedenleri tarihsel değişimi ile incelenmektedir. Ayrıca; DDoS saldırılarını gerçekleştirmekte kullanılan yöntemler, kategorize edilip örnekler ile anlatılmaktadır. DDoS 'un bir siber terör aracı olarak nasıl kullanıldığı açıklanmaktadır. Ayrıca, siber terörizm ile DDoS saldırıları arasındaki ilişki sunulmaktadır.

Cyber Terror and DDoS

Keywords
DDoS,
Cyber terror,
DDoS classification,
DDoS attack motivation

Abstract: DDoS is now used as an effective tool in cyber terrorism, however in the 1980s, script kiddies performed DDoS as a way to show off their abilities. It wasn't until the 1990s, that cyber criminals realized they could use these attacks to damage e-commerce companies. During this time, DDoS attacks were used as an extortion tool. In the new millenium, people began using these attacks as a tool for cyber protest. This study investigates the evolution of DDoS attack motivations, classifies the attack approaches, and explains them with examples. Also presents the connection between cyber terrorism and DDoS attacks.

1. Giriş

Ülkeler arası sınırlar sanal âlemle beraber yok olmaktadır. Ülkelerin; sosyal, ekonomik ve askeri alanlarda teknoloji kullanımı ve teknoloji bağımlılığı artmaktadır. Teknoloji kullanımının her alanda yaygınlaşması faydalarının yanı sıra riskleri de beraberinde getirir. İletişim teknolojisinin gelişmesiyle beraber saldırı kavramı da değişiklik göstermektedir. Günümüzde teknolojinin yaygın kullanıldığı sektörler ve kritik alt yapılara zarar vermek için bilgi ve iletişim altyapılarına yapılan saldırıların arttığı gözlenmektedir.

Türk dil kurumunun tanımına göre Terör; yıldırma, cana kıyma ve malı yakıp yıkma olarak tanımlanır. Terörizm ise bir siyasi davayı zorla kabul ettirmek için karşı tarafa korku salacak, cana ve mala kıyacak davranışlarda bulunma olarak tanımlanmaktadır [1]. Bu tanımlamalar rehberliğinde, bireylerin canına ve malına yönelik yapılan saldırıları, terör olarak değerlendirebiliriz. Geniş bant ağ teknolojisinin gelişmesi ile internet, insanların sosyalleştiği, ihtiyaçlarını giderdiği, sosyal ekonomik ve kültürel bir platforma dönüşmektedir. Bu platformda insanların düzenini bozacak saldırılar da gerçekleşmektedir.

Bu saldırılar ile beraber uluslararası arenada siber terör ve terörizm kavramları sıklıkla konuşulurken [2,3,4], ulusal literatürde bu alanda yapılan çalışmaların azlığı göze çarpmaktadır. Ülkemizde, akademik veri tabanının "siber terör" başlığı ile taranması sonucunda; Ekim 2018 itibari ile toplam 10 adet çalışma ile karşılaşılmaktadır [4-13] ve bu çalışmalardan 3 tanesi, siber terör konusuna teknik bakış açısı getirmektedir [5-7].

*İlgili yazar: sureyya.gulnar@gazi.edu.tr

"Siber saldırı" tanımı günümüzde gerek uluslararası platformda gerekse de ulusal platformda kesin olarak yapılamamaktadır [14]. Buna bağlı olarak "siber terör" kavramının, ortak kabul edilmiş bir tanımı bulunmadığından, ucu açık bir kavram olarak kabul edilmektedir [2]. Türk dil kurumunun terör tanımı ve bu saldırıların sayısal ortamlarda gerçekleştirildiği göz önünde bulundurulduğunda, siber terör; bireylerin veya toplumların can ve mal güvenliğini riske atmak/zarar vermek için etkileşimde bulundukları, sayısal teknolojilere ve/veya platformlara gerçekleştirilen saldırılar olarak tanımlanabilir.

Siber terör olarak adlandırılabilecek saldırılara bakıldığında aslında terör saldırıları ile aynı amaca hizmet ettiği görülmektedir. Sayısal ortamda gerçekleştirilen bu saldırılar ile bir mülke ciddi zarar verilebilir. Halkın sağlığı ve güvenliği için ciddi riskler ortaya çıkabilir. Ciddi ekonomik kayıp ve güvenlik ihlali meydana gelebilir. Bir ulusun sosyal ve politik istikrarı ve uyumu ciddi bir şekilde ihlal edilebilir [2]. Bu eylemler, saldırganların gözünden bakıldığında ise, bir sosyal hak olarak görülebilir iken [15], saldırıların bireysel hak ve özgürlükleri tehdit etmesi ve toplum düzenine zarar vermesinden dolayı eylemlerin bir terör saldırısı olarak kabul edilmesi de önerilmektedir [16]. Wray bu durumu; Elektronik Sivil İtaatsizlik (ESİ) olarak değerlendirmekte ve geleneksel sivil itaatsizlik eyleminde yer alan katılımcılardan farklı olarak, bir ESİ katılımcısı, evden, işten, üniversiteden ya da iletişim ağının diğer erişim noktalarından sanal engelleme ve oturma eylemlerine katılabilmektedir [17]. DDoS saldırılarını gerçekleştirenler genellikle bilinmemektedir. Fakat kimi zaman, hacktivist gruplar yapılan saldırıya sahip çıkmakta ve gerçekleştirilen saldırının sebebini açıklamaktadır. Bu saldırganlar günümüzde çoğu zaman DDoS'u araç olarak kullanarak gerçekleştirdikleri eylemleri bir sosyal hak olarak görüp, DDoS'u sayısal oturma eylemi (virtual sit-in) olarak tanımlamaktadır [16]. (D)DoS tartışmasız saldırganlar tarafından en çok kullanılan ESİ aracıdır [17]. Bu çalışmada; siber terör eylemlerinde bir araç olarak kullanılan DDoS saldırıları incelenmektedir. Ulusal literatür incelendiğinde Siber terör ve DDoS başlığı altında herhangi bir çalışma ile karşılaşılmamaktadır.

Günümüzde önemi her geçen gün artan DDoS saldırılarının kronolojik gelişimi dikkat çekicidir. Bu çalışmanın ana hedefi, siber terör aracı olarak kullanılan DDoS saldırılarının gerçekleştirilme sebeplerini incelemek ve DDoS saldırılarını gerçekleştirilme yöntemlerine göre sınıflandırmaktadır. Bu doğrultuda; Bölüm 2'de DDoS saldırılarının gerçekleştirilme nedenlerinin tarihsel değişimi incelenmektedir. Kronolojik inceleme sonucunda DDoS saldırılarının hangi amaçla başlatıldığı ve günümüze hangi amaçları gözeterek geldiği sunulmaktadır. Bölüm 3'de DDoS'u gerçekleştirmekte kullanılan yöntemler kategorize edilip örneklerle anlatılmaktadır. Makale; siber terör ve DDoS arasındaki ilişkinin değerlendirilmesi ile sonuçlandırılmaktadır.

2. DDoS Saldırılarının Gerçekleştirilme Nedenleri

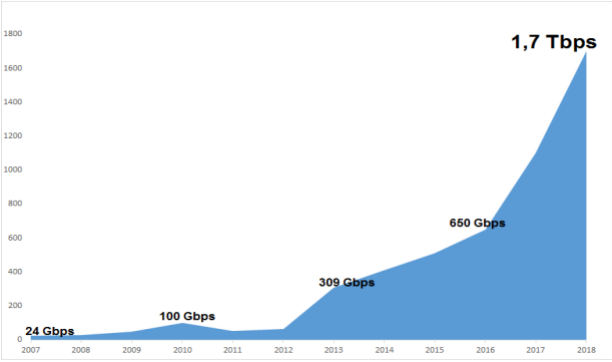
Geniş bant ağ teknolojinin ilerlemesiyle beraber internet artık hayatımızın vazgeçilmez parçası haline gelmektedir. Ayrıca, "akıllı" teknoloji kavramı günlük yaşamımızın her alanında karşımıza çıkmaktadır. Akıllı teknolojinin hızla gelişimine paralel olarak, ağa bağlı cihazların sayısı artmaktadır. Bu sebeple ağ tabanlı hizmetlerin aksaması veya kesilmesi iş ve işlemleri gerçekleştirme sırasında kişi veya kurumda ciddi mağduriyet oluşturmaktadır. DDoS saldırıları da bu sistem ve servislere karşı ciddi bir tehdit olarak görülmektedir. DDoS saldırganlarının, yetkinlikleri artmakta ve saldırganlar her geçen gün kendilerine yeni hedefler belirtmektedirler. Bu doğrultuda; DDoS saldırılarının geçmişten günümüze doğru incelenmesi saldırılar hakkında genel bir bakış açısı sunmaktadır. İlerleyen bölümlerde; DDoS saldırı boyutları ve DDoS saldırı nedenleri, kronolojik olarak değerlendirilmektedir.

2.1. DDoS saldırı boyutları

DDoS saldırılarının, meydana geldiği ilk zamanlarda saldırı boyutları düşük seviyedeydi. İlk yıllarda, saldırı boyutlarında aşırı bir değişim gözlemlenmedi. Fakat geniş bant teknolojisinin gelişimi, internet kullanım oranındaki artış, siber dünya da botnetlerin etkinleşmesi, güvenlik seviyesi düşük IoT cihazların ağda artması sonucu, saldırı boyutları da hızlı bir oranda artış gösterdi. DDoS saldırılarının, 2015 yılında yaklaşık olarak 500 Gbps seviyesine ulaştığı raporlanırken, 2016 da bu değer yaklaşık olarak 800 Gbps seviyesini buldu. Symantec internet güvenliği risk 2017 raporuna göre; Mirai botnetinin, Brian Krebs web sitesine yönelik yaptığı saldırı bu zamana kadar raporlanan en büyük DDoS saldırısıdır ve 620 Gbps seviyesini buldu. Hatta raporun yayınlandığı tarih olan Nisan 2017 de, Fransız hosting kurumu OVM, 1Tbps seviyesinde DDoS saldırısına maruz kaldı [18]. Arbornet 2018 kayıtlarına göre ise Mart 2018'de 1.7 Tbps gücünde saldırı tespiti yapıldı [19]. DDoS saldırılarının maksimum bant genişliği ve zamana bağlı değişimi Şekil 1'de görülmektedir.

2.2. DDoS saldırı nedenlerinin tarihsel gelişimi

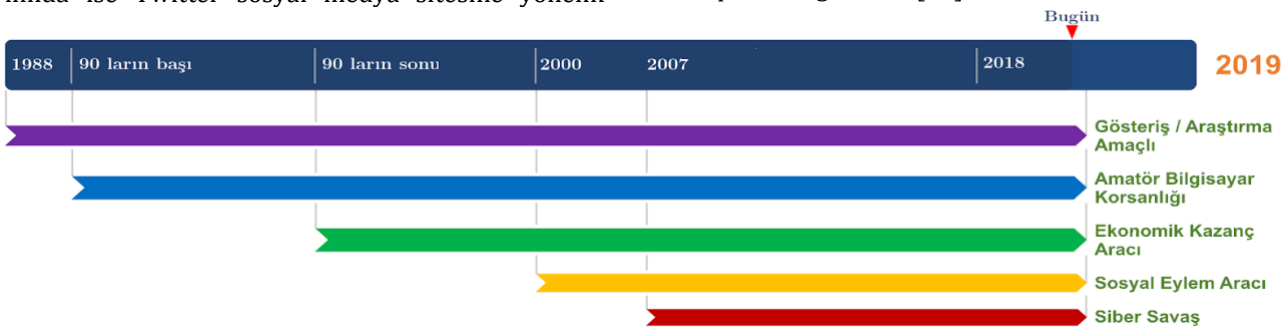
DDoS saldırılarının, gerçekleştirilme sebepleri kronolojik olarak incelendiğinde, saldırı motivasyonun beş temel evrede geliştiği gözlemlenmektedir. Bu saldırıların başlangıcı olarak bilinen 1988 yılında saldırının gerçekleştirilme nedeni merak ve eğlenceyken, günümüze gelindiğinde ise saldırıların motivasyonundaki değişimler Şekil 2' de gösterilmektedir. Bu bölümde; DDoS saldırılarının zaman içerisinde motivasyonundaki değişim detaylı olarak incelenmektedir.



Şekil 1. Raporlanan en yüksek DDoS saldırı boyutları [19]

Tarihte, bilgisayar dünyasında ilk hizmet engelleme saldırısı olarak bilinen morris virüsü, 1988 yılında Rober Tappan Morris tarafından eğlence amaçlı yazıldı. Morris'in, kodlama sırasında yaptığı bir yanlış sonucu ortaya çıkan bu program, Morris solucanı, sadece birkaç gün içinde günümüz İnternetinin öncüsü olan Arpanet'i gezdi ve internete bağlı olan bilgisayarların %10'unun ağlarını çalışmaz hale getirdi [20]. 1999 yılında, amatör bilgisayar korsanlarının DDoS' u araç olarak kullanılmasına örnek olan melissa virüsünün, kısa süre içerisinde bilgisayar ve elektronik posta sistemlerine vermiş olduğu zararın ise 80 milyon dolardan daha fazla olduğu tespit edildi [21]. Yeni millenyum ile beraber, DDoS saldırıları ciddi maddi kayıplara yol açmaya başladı. Yankee grubun çalışmasına göre 2000 yılının Şubat ayında Amazon, Yahoo, eBay gibi önemli sitelere karşı yapılan saldırıların yaklaşık olarak 1,2 milyar dolar zarara uğratıldığı tespit edildi [21]. 2001 yılının Eylül ayında ise Microsoft'un yaklaşık olarak 500 milyon dolar kaybettiği belirtildi [4]. DDoS saldırılarının sosyal eylem aracı olarak kullanıldığı 2010 yılında, Wikileaks internet sitesine yardım yasaklarından dolayı Mastercard, PayPal, Visa ve Postfinance internet siteleri DDoS saldırısına maruz kalarak belirli bir süre hizmet veremedi [5]. Anonymous, belirli bir yapılanmaya sahip olmayan hactivist bir gruptur ve sosyal protestolar için DDoS saldırılarını kullanan en bilindik örgütlerden birisi olarak tanımlanmaktadır [17]. Wikileaks, anonymous grubunun ilk gerçekleştirdiği eylem değildi. 2008 yılında Scientology Kilisesi'nin haksız olarak vergi muafiyetine sahip olduklarını düşündükleri için anonymous tarafından Scientology kilisesinin, internet sitesi DDoS saldırıları ile kullanılmayan hale geldi ve telefon hatları kilitlendi [22]. Ayrıca; 2009 yılında ise Twitter sosyal medya sitesine yönelik yapılan saldırı ile kullanıcılar twitter hesaplarına saatlerce erişemedi [23]. 2011 yılında ise Lulzsec adını kullanan saldırgan grup, CIA internet sitesinin sunucusuna erişip aşırı talep isteği göndererek CIA internet sitesini kullanılmaz duruma getirdi [24]. 2012 yılında ise Türk Hava Yolları çalışanlarının grevlerine destek olmak amacıyla Anonymous tarafından gerçekleştirilen saldırıda, Türk Hava Yolları çevrimiçi uçuşlar sayfası DDoS saldırısına uğradı ve uçuşlar bu sebeple gecikti [25].

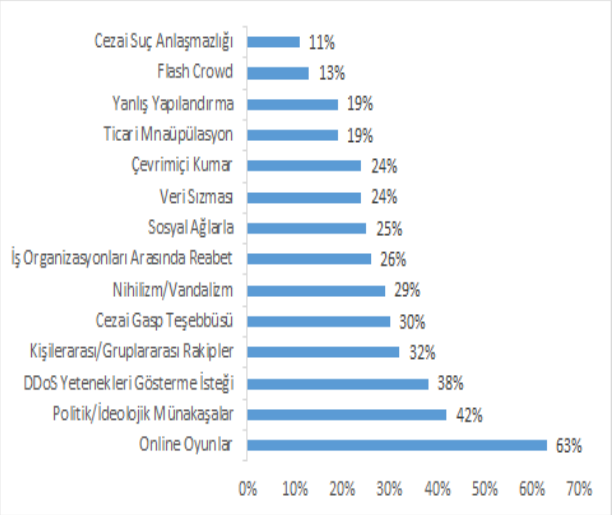
DDoS'un, 2007 yılında ilk defa Estonya'ya karşı siber savaş aracı olarak kullanıldığı kabul edildi. Estonya hükümeti, Sovyet döneminden Bronz heykeli taşıyınca Rusya duruma sert tepki gösterdi. Tam bu tarihlerde, siber saldırı ile önce siyasi hedefler seçen saldırganlar, sonra medya üzerinden halkın bilgi edinme olanaklarını kısıtladı ve bankacılık sektörünü, yani ekonomiyi hedef aldı. Estonya, saldırılara çözüm üretemeyince internet ile bağlarını geçici bir süre kesti. Saldırılar 3 hafta sürdü, tarihteki en büyük DDoS değildi, ama ilk defa suçlu spammer botnetler, bir ülkenin ulusal güvenliğini tehdit etti. Rus devleti sorumlu olarak görüldü fakat bu asla ispatlanamadı. Bu olayla birlikte, siber suçlar artık ulusal ve uluslararası güvenlik için olası bir tehdit haline geldi ve içerisinde bulunduğumuz sayısal dünyanın aslında savunmasız olduğu meydana çıktı [26]. Rusya ile Gürcistan arasında sınır şeridinde yer alan Güney Osetya bölgesi için 2008 yılında anlaşmazlık çıktı, cephede yaşanılan savaş sanal ortama taşındı. Gürcistan'da gerçekleşen DDoS saldırısı ile Gürcistan devlet kurumlarına ait sistemlere uzun süre erişilemedi [19]. 2012 yılında İran, Amerikan bankalarına, binlerce yüksek güçlü uygulama sunucusu içeren botnet kullanarak büyük bir DDoS saldırısı başlattı. Saldırgan, saniyede 60 gigabiti aşan seller oluşturmak için "itsoknoproblembro" olarak bilinen yeni bir araç kullandı. Önemli finans kurumları yavaşlama ve ara sıra görülen kesintiler yaşadı. En büyük üç ABD bankasına yönelik yapılan saldırıların İran'dan kaynaklandığı açıklandı ancak bu durum hiçbir zaman ispatlanamadı [27]. Ekim 2018 de İsveç'te gerçekleşen DDoS saldırısı sonucu trenlerinin sırasını düzenleyen bilgisayar programı çöktü. Saldırıdan sonra şirket bazı trenleri durdurdu bazı trenleri ertelemek zorunda kaldı ve rezervasyon durdu. Kasım 2015, İsveç hava trafiğine yapılan saldırı için, 2016 yılında İsveç yetkilileri Rusya'yı sebep olarak gösterdi [28].



Şekil 2. DDoS saldırı motivasyon

2.3. Günümüzde DDoS Saldırı Nedenleri

Günümüzde, DDoS saldırıları birçok amaçla gerçekleştirilmektedir. Saldırganlar; hobi amaçlı, kişisel hırsları yüzünden, finansal kazanım sağlamak için, ideolojik yaklaşımlarından dolayı saldırı yapabilmektedir. Genel trendlerin yanısıra, 2017 yılında Arbornet'in yayınlamış olduğu güvenlik raporu, saldırganların hangi amaçla ve hangi yollarla DDoS saldırılarını gerçekleştirdiğini Şekil 3 üzerinden güncel verilerle sunar [19].

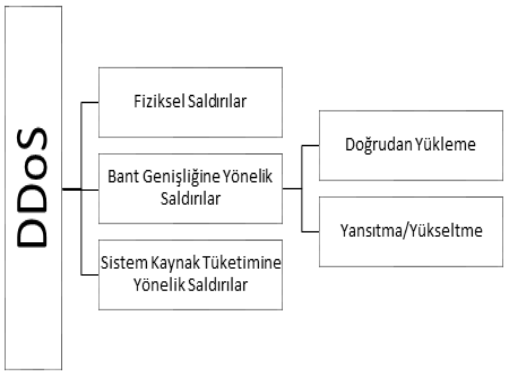


Şekil 3. Günümüzde DDoS Saldırı Nedenleri [19]

3. DDOS Saldırıları Gerçekleştirilirken Kullanılan Yöntemler

Bir ağa bağlı bilgisayar sistemlerinin veya kaynaklarının aşırı kalabalıklaşmasını ve bu kalabalıklaşma sonucunda yasal olmayan hizmetlerin gerçekleşmesini amaçlayan tehditler, genellikle Hizmet Reddi (DoS) saldırıları olarak adlandırılır [29]. Hizmet reddi saldırıları ile sistemin ağ üzerinden hizmet alması engellenir. Zombiler veya botlar olarak adlandırılan makinalar grubu harekete geçerek, hedef sistemin CPU, bellek veya bant genişliği gibi ağ kaynaklarını tüketmek için hedef sisteme koordineli trafik gönderir.

DDoS saldırılarının dağıtık yapısından dolayı saldırı trafiği ve gerçek trafik ayrımını yapmakta oldukça zordur [30]. Günümüzde DDoS saldırıları İnternet hizmetlerinin kullanılabilirliğini engellemek için saldırgan tarafından tercih edilen en güçlü silah olarak kabul edilmektedir [31]. Literatürde yapılan çalışmaların incelenmesi sonucunda; DDoS saldırılarının, farklı araştırmacılar tarafından farklı ölçütlere göre sınıflandırıldığı gözlemlenmektedir. Bu çalışmada; DDoS saldırıları, hedefe zarar verme yöntemlerine bağlı olarak sınıflandırılmaktadır. DDoS saldırı sınıfları, fiziksel saldırılar, bant genişliğine yönelik yapılan saldırılar ve sistem kaynakları tüketimine yönelik yapılan saldırılar olmak üzere üç ana kategoride Şekil 4'de gösterildiği gibi incelenmektedir. Aşağıda yer alan bölümlerde bu üç kategoriye ait olan DDoS saldırıları teknik olarak tanımlanmakta ve incelenmektedir.



Şekil 4. DDoS saldırı türleri

3.1. Fiziksel saldırılar

Fiziksel DDoS saldırılarında, fiziksel olarak hizmetin engellemesi veya sekteye uğratılması ana hedeftir. Bu müdahale doğrudan veya dolaylı olarak gerçekleştirilebilir. Bir sistemin çalışması için gerekli altyapıya yapılacak fiziksel bir müdahale veya bu altyapıya uzun vadede zarar verecek sistem ayarlarındaki değişiklikler fiziksel saldırı sınıfında sayılabilir. Almanya'da gerçekleşen DDoS saldırısı, fiziksel saldırıların önemine dair en iyi örneklerden birisidir. Almanya'da bir demir çelik üretim fabrikasının bilgisayar sistemi kötücül bir yazılımla, saldırganların eline geçti, yüksek sıcaklıkta olan fırınların yazılımlarıyla oynandı ve bu sayede üretim durduruldu [32]. İran nükleer santraline yönelik yapılan fiziksel saldırı ise santral santrifüjlerinin dönüş hızı, Stuxnet isimli kötücül bir yazılım yardımı ile azaltılarak, uzun sürede üretim aksaması gerçekleşti [28]. New York'ta bulunan Bowman Avenue Dam adlı baraja yapılan saldırı da ise, saldırı anında kanal kapısının elle kontrol ediliyor olmasından dolayı fiziksel bir hasar meydana gelmedi. Saldırganların amacı kanal kapağını istediği zaman açabilmekti, eğer kapak, saldırganlar tarafından açılabilmiş olsaydı 200 konutu etkileyebilecek kötü bir durumla karşı karşıya kalınacaktı [31].

3.2. Bant genişliğine yönelik yapılan saldırılar

DDoS saldırıları; bant genişliğini tüketmeye yönelik yapılıyor ise volümetrik (hacimsel) saldırılar adını almaktadır. Volumetrik saldırılar, kötü amaçlı yazılım (malware) bulaşmış sistemler vasıtası ile doğrudan veya halka açık ağ servislerini suistimal edip yansıtma/yükseltme yapılarak gerçekleştirilebilir.

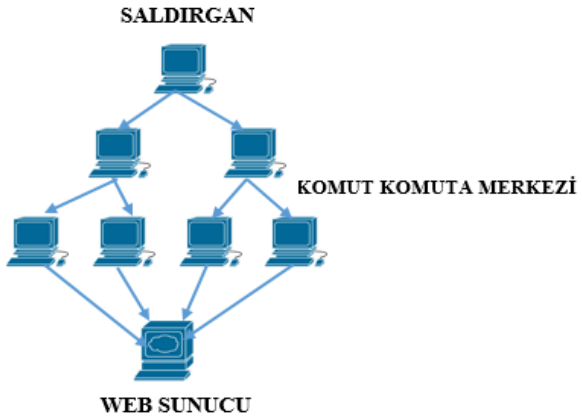
Siber saldırganlar, kötü amaçlı yazılım bulaşmış cihazları uzaktan kontrol ederek, hedefe giden yolda trafik akışını artırarak, hedefte hizmet aksamasına veya engellenmesine sebep olabilirler. Genellikle botnet (robot network) olarak adlandırılan, bu uzaktan kontrol edilebilir ağlar; kontrolü ele

geçirilmiş bilgisayarlar, sunucular ve benzeri ağ cihazları kullanarak DDoS saldırılarını gerçekleştirmektedir.

Volümetrik saldırılarda saldırgan, saldırı yapacağı ağa botnetler yardımı ile çok fazla sayıda paket göndererek ağın bant genişliğinin taşmasına sebep olmaktadır. Böyle bir saldırıda, Internet Kontrol İletisi Protokolü (ICMP), Kullanıcı Veri Bloğu Protokolü (UDP) ve İletim Denetimi Protokolü (TCP) gibi farklı ağ katmanı protokolleri kullanılabilir [30]. Volümetrik saldırıların büyüklüğü genellikle saniyede bit veya paket olarak ölçülmektedir. Arbor Network'ün 2017 yılında yayınladığı internet güvenliği raporuna göre, DDoS saldırılarının % 65'i volümetrik niteliktedir [20]. Volümetrik saldırılar, gerçekleştirilme yöntemlerine göre doğrudan ve yansıtma/yükseltme (reflection/amplification) saldırıları olarak iki kategoride incelenmektedir.

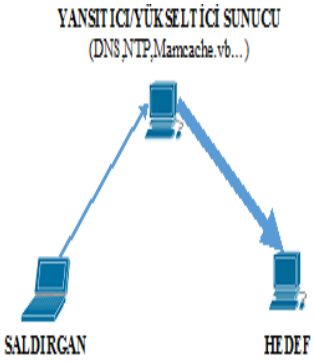
Doğrudan gerçekleştirilen DDoS saldırılarında, saldırgan, saldırı komutunu, komut komuta merkezine (C&C) iletir, komut komuta merkezi, kontrolü ele geçirilmiş ağ cihazlarına hedefe yönelik trafik göndermesi için komut verir [29]. Bu sistemde yer alan katmanlı yapı ile saldırganın kimliği gizlenir ve böylece kaynak hakkında ipucu bulunamaz [33]. Bu yöntemle oluşturulan yüksek seviyedeki trafik hacmi, hedefin bant genişliğini kaplamakta ve hedefte hizmet aksamasına veya engellenmesine sebep olmaktadır.

Doğrudan saldırıların nasıl gerçekleştiğini Şekil 5 en basit anlamda göstermektedir. Doğrudan saldırılara; ICMP sel, UDP sel örnek olarak verilebilir. Günümüzde bilinen yüksek hacimli sel saldırıları, güvenlik seviyesi düşük IoT cihazlarını kullanan Mirai botneti aracılığı ile gerçekleştirilmiştir [34].



Şekil 5. Doğrudan volümetrik DDoS saldırıları

Hedefin bant genişliğine yansıtma/yükseltme yöntemi ile yapılan saldırılar Şekil 6' da gösterilmektedir. Saldırgan bu saldırılarda herkes tarafından kullanılabilen, zafiyeti bulunan sunucuları bir yükseltme/yansıtma aracı olarak kullanır. Yansıtma/Yükseltme aracı olarak kullanılan bu sunucular; herkes tarafından erişilebilmektedir. Bu sunuculara DNS, NTP, Memcache örnek olarak verilebilir. Saldırgan; sahteleştirdiği paketleri sunucuya gönderir. Yansıtıcı/Yükseltici ise paketleri kendi üzerinden hedef bilgisayara gönderir. Bu işlemi gerçekleştirirken paketler sunucu üzerinden yansıtılmış veya yükseltme faktör değerine göre yükseltilmiş olarak gönderilir. Sonuç olarak fazlalaşan paket sayısı ile birlikte hedefin bant genişliğinde taşma meydana gelir ve hedefte hizmet aksar veya kesilir.



Şekil 6. Yansıtma/yükseltme volümetrik DDoS saldırıları

Yansıtma saldırılarında, saldırganlar, saldırı trafiğini hedefe göndermek için reflektör adı verilen bileşenden faydalanmaktadır. Saldırgan sahte IP kullanan paketleri, reflektör görevi gören ve ara katman olarak kullanılan bilgisayarlara gönderir. Yükseltme saldırılarında ise ara katman olarak kullanılan bileşen amplifikatör adını alır ve hedefe gönderilen paketler, kullanılan protokole bağlı olarak farklı oranlarda yükseltilmektedir. Bu yükseltme katsayısı; yükseltme faktör değeri olarak adlandırılmaktadır. Yükseltme faktör değeri, yansıtma/yükseltme DDoS saldırılarında önem taşımaktadır. Bu yükseltme katsayısı; yükselticiden hedefe giden paket boyutunun, saldırgandan yükselticiye giden paket boyutuna bölünmesi ile hesaplanmaktadır. Yansıtma/Yükseltme saldırılarında kullanılan protokoller ve bu protokollerin yükseltme katsayıları Tablo 1'de gösterilmektedir [35]. Günümüzde gerçekleşen saldırılarda genellikle yansıtma ve yükseltme saldırıları aynı anda gerçekleştirilmektedir. Bu saldırılara örnek olarak; Smurf, Fraggle, NTP Amplifikasyon, DNS Amplifikasyon, Memcache Amplifikasyon verilebilir. Smurf saldırılarında; ICMP echo istekleri (ping) yayın adreslerine gönderilir. ICMP echo isteği alan aygıt bağlı olduğu her bir cihaz ile sahte kaynak adrese echo yanıtı gönderir. Fraggle saldırılarında, bir ağdaki bir yönlendiricinin yayın adresine çok miktarda sahte UDP trafiği gönderilerek hizmet engellenir. Fraggle saldırıları, Smurf saldırılarına çok benzer fakat 1999 tarihinden itibaren yönlendiriciler yayın adreslerine yönlendirilen paketleri iletmedikleri için çoğu ağ artık Smurf ve Fraggle saldırılarına karşı tedbirlidir [35].

Tablo 1. Kullanılan protokollere bağlı yükseltme katsayıları

Protokol	*Yükseltme Katsayısı*
NetBios	3.8
BitTorrent	3.8
SNMPv2	6.3
DNS	28-54
NTP	556.9
Memcache	10.000 – 50.000

NTP, internet'e bağlı makinaların saatlerini ayarlamak için kullandığı ağ zaman protokolüdür. NTP amplifikasyon saldırılarında DDoS saldırganı NTP selinden yararlanır. Saldırgan, NTP altyapısını aldatmak için, açık olan NTP sunucuları yardımı ile ağ da sel oluşturur [36], DNS (alan adı sistemi) internet sitelerinin isimlerini IP adreslerine yönlendiren bir veritabanına sahip sunucu bilgisayar olarak tanımlanabilir. DNS amplifikasyon saldırısı; saldırganın kurbanın açık olan bir DNS çözümleyicisine sahte bir IP adresi kullanarak DNS sorgusu yapması ile başlar. Saldırgan tarafından botnetler aracılığı ile çok sayıda sahte sorgunun gönderilmesi ve birkaç DNS çözümleyicinin aynı anda yanıt vermesi ile hedef ağda hizmet aksaması meydana gelir [37]. NTP amplifikasyonu ve DNS amplifikasyonu gibi DDoS amplifikasyon saldırılarına benzer şekilde çalışan Memcache saldırıları da, amplifikasyon saldırılarına örnektir. Memcache; web sitelerini ve ağları hızlandırmak için kullanılan bir veritabanı önbellekleme sistemidir [34]. Memcache sunucuları, UDP protokolünü kullanarak çalışma seçeneğine sahiptir. UDP protokolünde paketler, alıcı taraftan cevap beklemeden gönderilir. Saldırgan, hedefin IP adresinden geliyormuş gibi UDP taleplerini memcache sunuculara gönderir. Memcache sunucuların temel özelliğinden kaynaklı olarak, cevap talebe göre kat kat büyür. Bu yükseltilmiş cevaplar hedefin web sitesine doğru büyük miktarda gereksiz trafik oluşturur. Bu sayede hedefte hizmet akaması veya engellemesi meydana gelir.

3.3. Sistem kaynaklarının tüketimine yönelik yapılan saldırılar

Sistem kaynaklarını, sabit disk, işlemci, geçici bellek tüketimi için protokol zafiyetlerinden faydalanılarak gerçekleştirilen DDoS saldırılarıdır. Bu saldırılar da ağa gönderilen yüksek paket sayısı bulunmamaktadır. Bu saldırılara; Fork Bomb, HTTP GET/POST, slowloris örnek olarak verilebilir.

Fork Bomb; çatal bomba olarak bilinen DDoS saldırısı; sistemin CPU ve bellek tüketime yönelik sistem zafiyetlerinden faydalanılarak yapılır. Unix ve Linux sistemlerinde var olan bir işlemi tekrar tekrar çalıştırma mantığına dayanır. Saldırının arkasında yatan temel fikir ise bir işlemin (process) kendi başına yeni kopyalarını tekrar tekrar başlatması ve sonsuz bir döngü oluşturması ile işlemciyi ve belleği yormaktır. Microsoft Windows işletim sistemlerinin Unix fork sistem çağrısına eşdeğer bir işlevi olmadığı için bu saldırı Microsoft Windows işletim sistemlerinde yapılamaz [36].

HTTP istemcisi bir sunucuya HTTP isteğini, genellikle GET veya POST çağrılarını kullanarak gönderir. Post istekleri dinamik olarak oluşturulmuş kaynaklara erişmek için kullanırken, GET isteği resimler gibi standart ve statik içeriği almak için kullanılmaktadır. Saldırgan genellikle sunucuyu, mümkün olduğunca çok işlem gerektiren yoğun istek göndererek meşgul eder. HTTP GET sel saldırıları uygulama katmanına yönelik yapılan en popüler DDoS saldırılarından birisidir [37].

TCP, günümüzde en çok kullanılan iletişim protokolüdür. TCP protokolünün zafiyetlerinden faydalanan saldırganlar, uygulama katmanı DDoS saldırılarını kolaylıkla gerçekleştirebilir. Uygulama katmanına yönelik, kaynak tüketimini hedef alarak yapılan saldırılara; slowget, slowpost, slowloris örnek olarak verilebilir. Uygulama katmanına yönelik yapılan DDoS saldırılarında kaynak tüketimi, hafızada daha fazla yer tutma işlemine dayalı olarak gerçekleştirilir. Sürekli gönderilen istek mesajı ile beraber sistem belleğinde oluşan kuyruk nedeniyle hedef, isteklere cevap veremez duruma gelir. İstemci sunucudan gelen veriyi yavaş okuduğunda ve/veya istemci sunucuya veriyi yavaş gönderdiğinde sunucu kaynakları gereğinden uzun süre meşgul edilir [29].

4. Sonuç

DDoS saldırılarının, ilk gerçekleştirildiği günden bu yana yıkıcı etkileri artarak devam etmektedir. DDoS saldırılarının gerçekleştirilme nedenleri tarihsel olarak incelendiğinde günümüze kadar beş farklı amaca hizmet ettiği gözlemlenmektedir. İlk başladığı yıllarda saldırılar, gösteriş/araştırma amaçlı gerçekleştirilirken daha sonradan saldırı sebeplerinde değişiklik gözlenmektedir. Saldırıların ilerleyen zaman içerisinde eylem aracı ve siber savaş aracı olarak kullanıldığı bilinmektedir ve bu eylemlerin bir bireysel hak mı yoksa suç mu olduğu hala tartışılmaktadır. Bu değerlendirmenin yapılabilmesi için siber suç ve suç teşkil edebilecek eylemlerin net olarak tanımlaması ve gerekli yasal düzenlemelerin yapılması gerekmektedir. Siber teröristler birçok farklı saldırı yöntemi kullanmaktadır. Bunlardan bazıları; ağa sızma, virüsler, solucanlar, malwarelar, phishing ve DoS / DDoS olarak sıralanabilir. (D)DoS sistemlerin hizmetlerinin aksaması veya engellenmesine yönelik, sisteme fiziksel zarar vererek veya sistemin bant genişliğinde taşma meydana getirerek ya da sistemin kaynaklarını tüketmeye yönelik gerçekleştirilmektedir.

DDoS saldırılarının gerçekleştirilme nedenleri ile paralel olarak saldırıların boyutlarında da ciddi artış

gözlenmektedir. Saldırıların boyutu ilk zamanlarda Megabyte seviyelerinde iken günümüzde Terabyte seviyelerine ulaşmaktadır. Bu çalışmada, siber terör olarak adlandırılan Elektronik Siber İtaatsizlik eylemlerinin en popüler araçlarından biri olan DDoS saldırılarının motivasyonunun tarihsel evrimi incelenmiştir. Ayrıca DDoS saldırıları, hedefe zarar verme yöntemlerine bağlı olarak sınıflandırılıp örnekler ile anlatılmıştır.

Kaynakça

[1] TDK sözlük, 2018. Terör. http://www.tdk.gov.tr (Erişim Tarihi: 10/10/2018).

[2] Sarah G., Richard F. "Cyberterrorism ?" 2002, Computers & Security, 21 (7), 636-647.

[3] Bozdemir, N. Z. 2016. "Re - Conceptualizing Cyberterrorism: Towards a New Definitional Framework." Ankara Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, 90s, Ankara.

[4] Luiijf E. 2014. "Definitions of Cyber Terrorism, Cyber Crime and Cyber Terrorism Investigator's Handbook", Bölüm 2, Syngress, 11-17.

[5] Sağıroğlu Ş. 2017. "Dünyada ve Ülkemizde Siber Terör ve Güvenlik," TÜBAV Konferansları, Ankara.

[6] Göztepe K., Ejder K, A. 2017. "Siber Terör Saldırılarından Korunmaya Yönelik Bulanık Mantık Tabanlı Karar Destek Modeli" Siber Güvenlik Çalıştayı, Ankara.

[7] Efe A. 2017. "Siber Teröre Karşı Siber Güvenlik COBIT 5 ve CSX", Gazi Üniversitesi Siber Terörle Mücadele Konferansı, Ankara.

[8] Hatipoğlu C. 2017. "Teknolojik Savaşlar Siber Terörizm Tehditleri" International Congress on Political, Economic and Social Studies (ICPESS), Ankara.

[9] Kara O., Aydın Ü., Oğuz A. "Ağ Ekonomisinin Karanlık Yüzü Siber Terör", 2006. 5. Bilgi, Ekonomi ve Yönetim Kongresi, İstanbul.

[10] Atıcı B. 2005. "Yeni Eğilimler ve Olanaklar Işığında Siber Terör", İstanbul Conference on Democracy and Global Security.

[11] Güntay V. 2014. "Karadeniz Ülkeleri Güvenliği Bağlamında Siber Terörizm ve Uluslararası İlişkiler", VI. Karadeniz Uluslararası Sempozyumu: Karadeniz'den Hazar'a Stratejik Bakış.

[12] Erdoğan Ö. 2013. "Siber Terörün Başedilemez Yıkıcılığı", Ekonomi, İş Dünyası ve Politika Dergisi, 60, 80–82.

[13] Atıcı B., Çetin G. 2003. "Sanal Ortamda Gerçek Tehditler Siber Terör ", Polis Dergisi, 37, 57–66.

[14] Önok M. 2013. "Avrupa Konseyi siber suç sözleşmesi ışığında siber suçlarla mücadelede uluslararası işbirliği" Marmara Üniversitesi Hukuk Araştırmaları Dergisi.

[15] Bartels, R. 2015. "The virtual sit-in" Master Political Science: The Philosophy of Inequality, Leiden University, 43s.

[16] Wray, S. 1998. "Electronic Civil Disobedience and the World Wide Web of Hacktivism:A Mapping of Extraparliamentarian Direct Action Net Politics". In Switch, 4.

[17] Olson, P. 2012. "We Are Anonymous – Inside the Hacker World of LulzSec, Anonymous, And the Global Cyber Insurgency", Little Brown, 423.

[18] Internet Security Threat Report. 2017. Symantec, 22.

[19] Arbour Networks, 2017. "Current DDoS attacks", http://www.asiapacificsecuritymagazine.com/wp-content/uploads/2017/01/2017-01-19-Arbor-WISR-Full-Report.pdf.

[20] Findingdulcinea. 2018. On This Day: Robert Tappan Morris Becomes First Hacker Prosecuted for Spreading Virus. http://www.findingdulcinea.com/news/on-this (Erişim Tarihi: 05/10/2018)