DDoS Saldırısı ve Failin Cezai Sorumluluğu

Gürkan Özocak

ÖZET

20. yüzyılın son döneminden itibaren, gelişen teknoloji ve bu gelişimle beraber ortaya çıkan "bilişim toplumu" ile birlikte, suç ve suçlulukla mücadele yöntemleri de değişmiş, ceza kanunlarında "bilişim suçları" adı verilen yeni bir suç topluluğu ortaya çıkmıştır. Türk ceza hukukunda da bilişim suçları, 5237 sayılı Türk Ceza Kanunu'nun 243 – 246. maddeleri arasında düzenlenmiştir. Özellikle son yıllarda en sık görülen bilişim suçu olan DDoS (*Distributed Denial of Service)* saldırısı, kısaca, saldırganın önceden ele geçirdiği *zombi* bilgisayarlar yoluyla bir hedef sisteme aynı anda çok sayıda istek göndererek, o hedef sistemin işleyişinin engellenmesidir. Failin, hedef bilişim sisteminin içerisine girmeyerek sadece sistemin hizmet verememesine sebep olduğu DDoS saldırısında, TCK m. 244 kapsamında cezalandırılması gerekmektedir.

Anahtar Kelimeler
Ceza Hukuku, Bilişim Hukuku, Bilişim Suçları, DoS ve DDoS Saldırısı.

SUMMARY

Beginning from recent periods of 20th Century, methods of struggle with crime and criminalism have been changed together with developing technology and information society, and a new group of crime named as "*cyber crimes*" have appeared in penal codes. In Turkish criminal law, cyber crimes are regulated in between Art. 243 – 246 of Turkish Penal Code (TCK) no. 5237. DDoS (*Distributed Denial of Service)* Attack, which is especially appeared in recent years, briefly, is preventing the functioning of a system by sending a large number of requests at the same time using the zombie computers that is seized by the perpetrator. DDoS Attack, that only the target system does not work, causes the perpetrator can be punished according to Art. 244 of TCK.

Keywords
Criminal Law, Informatics Law, IT Law, Cyber crimes, DoS and DDoS Attack.

GİRİŞ

Son yıllarda teknolojinin gelişmesiyle birlikte, işlenen suç tipleri de değişmekte ve bilişim yoluyla işlenen suçların sayısı günden güne artmaktadır. Bilişim ve özellikle bilgisayar sistemlerinin yaygınlaşması ile beraber ceza hukuku alanında, bu sistemlerin kötüye kullanımlarına ilişkin fiillerin cezalandırılabilirliği konusu gündeme gelmiş ve son dönem ceza kanunlarının hepsinde "*bilgisayar suçları*", "*bilişim suçları*" veya "*siber suçlar*" olarak adlandırılan suç tipleri düzenlenmiştir [1]. Bu husus 2004 tarihinde yürürlüğe giren ve Kasım 2010 itibariyle Türkiye'nin de tarafı haline geldiği "Avrupa Konseyi Siber Suç Sözleşmesi"nde de düzenlenmiş olup, Sözleşmenin 4, 5 ve 6. Maddelerinde, "Veriye Müdahale", "Sistemin Engellenmesi" ve "Cihazların Kötüye K

5237 sayılı Türk Ceza Kanunu'nda da, bilişim yoluyla işlenebilen klasik suçların dışında, 243 – 246. maddeler arasında "*Bilişim Alanında Suçlar*" başlığı altında, söz konusu suçlar öngörülmüştür. TCK m. 243 bilişim sistemlerine yetkisiz erişimi düzenlerken, TCK m. 244'de ise, bir bilişim sisteminin engellenmesi, bozulması, burada yer alan verilerin yok edilmesi veya değiştirilmesi fiilleri suç olarak düzenlenmiştir [2]. Ne var ki, kanunun genel ve soyut tanımını verdiği bu suçlar "*serbest hareketli suçlar*"dan olup, özellikle teknolojinin ilerlemesiyle doğru orantılı olarak, bu suçların işlenmesinin sayısız yolu ortaya çıkmaktadır. Nitekim, yine birçok eylemi kapsamına alan TCK m. 244'teki *"bilişim sisteminin engellenmesi"* fiilinin en çok ortaya çıkan yöntemlerinden birisi de DDoS Saldırısı yöntemidir.

DDOS SALDIRISI VE DDOS SALDIRISININ TÜRK CEZA KANUNU BAKIMINDAN DEĞERLENDİRİLMESİ

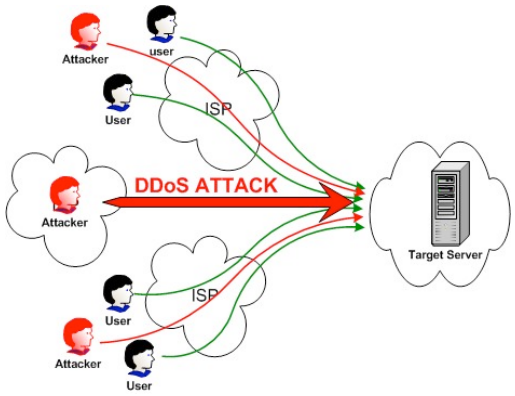
DoS ve DDoS Saldırısı Nedir

Bilişim alanında en çok görülen siber saldırıların başında DoS *(Denial of Service)* ve DDoS *(Distributed Denial of Service)* saldırıları gelmektedir. DoS saldırısı, kısaca, belli bir sunucunun belli bir şekilde hizmet bekleyen kullanıcılara hizmet verememesini sağlamak amacıyla, o bilgisayarın işlem yapmasını engellemek, bir başka deyişle hedef bilgisayarı bilişim sisteminin içerisine girmeksizin kilitlemektir. DoS işlemi, birden çok sayıda bilgisayar üzerinden yapıldığında, yani "dağıtılmış" (*distributed*) bir şekilde gerçekleştirildiğinde ise ortaya DDoS saldırısı çıkmaktadır [3].

DDoS saldırısında, saldırgan, *hacking* yoluyla daha önceden ele geçirmiş ve hazırlamış olduğu birçok makina üzerinden, seçmiş olduğu hedef sistemin trafiğini arttırarak, o sistemin işleyemez hale gelmesini sağlamaktadır. Saldırganın *hacking* yoluyla ele geçirmiş olduğu ve görünürde hedef bilgisayarların sistemlerine saldıran bu makinalara "*zombi*" adı verilir. *Zombi*ler esasen saldırganın daha önce bir açığını bularak ele geçirdiği (*hack* ettiği) ve saldırı sırasında kullanmak üzere içlerine program yerleştirdiği bilgisayarlardır. Bir başka deyişle, *zombi*ler saldırının merkezinde bulunan, ancak saldırı fiilinden haberdar dahi olmayan ve güvensiz olduğu için saldırgan tarafından ele geçirilmiş makinalardır. *Zombi* programları, genellikle güvenliği zayıf olan sistemlere yerleştirilir [4].

Saldırgan tarafından *zombil*er üzerinde kurulan programlar (*daemon*) belirli bir kaynaktan gelecek DDoS komutlarını dinlemekte ve bu yolla hedef sisteme saldırıları gerçekleştirmektedir. Binlerce bilgisayara yerleştirilen bu programlar, bilgisayarlara uzaktan kontrol (*remote*) imkanı vermekte, böylece saldırganın bu bilgisayarlar üzerinden istediği *server*'a istediği sayıda veri göndererek o *server*'ı çalışamaz hale getirmesine olanak sağlamaktadır [5].

İfade ettiğimiz gibi saldırgan, bu *zombi* bilgisayarları kullanarak hedef olarak belirlediği sisteme (bilgisayara ya da *hosta*) aynı anda giriş yapmaya çalışmakta ve bu yolla kapasitesinin çok üzerinde istek gelen sistem tamamen kilitlenerek çalışamaz hale gelmektedir. Örneğin, barındırma hizmeti veren bir firmadan belirli bir bant genişliği edinen ve buna göre azami olarak aynı anda 2 bin kişinin girebileceği bir web sitesine, aynı anda 20 bin kişinin girmeye çalıştığı ve girmeye çalışırken bu 20 bin kişinin ayna anda komut yolladığı durumda, bu web sitesine ulaşılması mümkün olmamaktadır. İşte DDoS saldırısı, aynı anda binlerce kişinin belli bir sisteme sürekli giriş yapmaya çalışması gibi, bu işi otomatize eden bir yazılımla hedef sistemi kilitlemekte ve çalışamaz duruma getirmektedir [6].



Şekil 1. DDoS Saldırı Şeması [7]

Yukarıdaki şemadan da görülebileceği üzere, DDoS saldırısında hedef sunucuya (*target server*), aynı anda çok sayıda istek gelmekte olup, sistemin kaynakları (*CPU, Stack, band vs*.) bu yoğun istekleri karşılayamadığı durumda, sisteme gerçek kullanıcılar (*user*) tarafından da erişilmesi imkansız hale gelmektedir. Sistemin bu kilitlenmesi durumu, *zombi* bilgisayarların çokluğuna ve gelen isteklerin yoğunluğuna bağlı olarak, saatler sürebilmekte olup, sisteme gelen yükün azalıp sisteme girişin kabul edilebilir seviyeye inmesine kadar devam edebilmektedir.

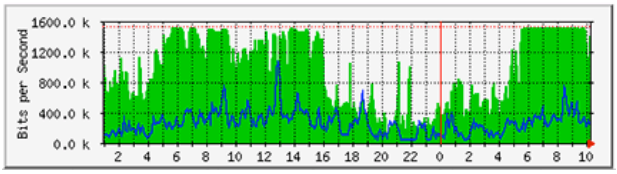
Koordineli bir biçimde yapılan bu işlem, hem saldırının yoğunluğunun artmasına, hem de gerçek saldırganın kimliğinin gizlenmesine yol açmaktadır. Zira, saldırılar *zombi* bilgisayarlar üzerinden yapıldığından, saldırı yapan bilgisayara ulaşılmak istenildiğinde *zombi* bilgisayarların IP adresleriyle karşılaşılmakta ve teknik olarak saldırıya katılmayan gerçek saldırgana ulaşmak mümkün olmamaktadır. Saldırı tek bir IP adresi üzerinden yapıldığında bir *Firewall* bunu rahatlıkla önleyebilecekken, daha çok sayıdaki IP adresinden saldırı yapılması, *log* taşması nedeniyle *Firewall* servislerini durdurmakta ve *Firewall*'un devre dışı kalmasına neden olmaktadır. İşte, DDoS saldırılarını, tek bir IP adresi üzerinden gelen DoS saldırılarından ayıran en önemli fark buradan kaynaklanmaktadır. DDoS saldırılarında, saldırgan çok sayıdaki *zombi* bilgisayarı hedef sisteme yönlendirdiğinden *Firewall* devre dışı kalmakta ve saldırının yoğunluğuna bağlı olarak önlenmesi kimi zaman imkansız hale gelmektedir [8].

DDoS Saldırısı Yöntemleri

Bant Genişliğine Yönelen Saldırılar

Bant genişliğine yönelen DDoS saldırıları, hedef sistemin sahip olduğu hattın doldurulması yoluyla gerçekleştirilmektedir. Bu saldırı türünde saldırgan hedef sisteme çok fazla sayıda istek gönderir; eğer gönderilen

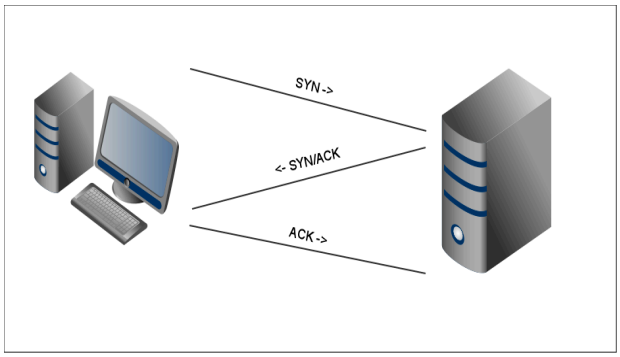
istekler hattın dolmasına yetmezse, bu kez dönen cevaplarla hat doldurulup sistem kilitlenmeye çalışılır. Örneğin, yüksek miktarda hat kapasitesine sahip bir İnternet sitesine gönderilecek istekler hattın dolmasına yetmeyebilir. Bu durumda, çok fazla sayıda kullanıcı, İnternet sitesi üzerindeki büyük bir dosyayı (*resim, video vb*.) çağırarak sunucudan dönen cevapların hattı doldurmasını ve gerçek kullanıcı isteklerine yer kalmamasını sağlayabilir.



Şekil 2. Bir Bant Üzerindeki Hat Kullanımı Grafiği [9]

Yukarıdaki grafik, bir sisteme ait hat kullanımının zamana bağlı olarak değişimini göstermektedir. Buradan görülebileceği üzere, özellikle saat 6 ila 10 arasında sistem maksimum hat kapasitesine ulaşmış ve hat tamamen dolmuştur. Buna hattın *sature* olması adı verilmektedir. Hattın *sature* olması durumunda, hedef sisteme mevcut trafiğin yanında yeni trafik gelemez, gelse de sistemden yanıt alması beklenen süreden çok daha uzun zaman alacak, böylece sistem çalışamaz yahut beklenenin çok altında performansla çalışır hale gelecektir.

SYN-Flood Saldırıları



Şekil 3. TCP Bağlantısı *(Üçlü El Sıkışma)* [10]

Bilgi Ağı üzerindeki bilgi iletimi ve paylaşımı işlemleri belirli kurallar dahilinde yapılmakta olup, bu kurallara kısaca TCP/IP (*Transmission Control Protocol/Internet Protocol*) protokolleri denilmektedir. Bunlar, bilgisayarlar ile veri iletme veya alma birimleri arasında koordinasyon sağlayan, bu şekilde bir yerden diğerine veri iletişimini sağlayan protokollerdir [11].

Yaygın bir DDoS yöntemi olan *SYN-flood* tekniğinde, saldırıların temelinde TCP'nin yapısı yatmaktadır. TCP bağlantısı 3 aşamada kurulmaktadır (Bu bağlantı silsilesine *üçlü el sıkışma* adı da verilmektedir). Yukarıdaki şemada da gösterildiği gibi, birinci aşamada istemci makina, sunucu makinanın portuna bağlanmak için bir istek gönderir (SYN), ikinci aşamada sunucu makina koşullar uygunsa bu isteği kabul eder ve istemciye bir onaylama (*Acknowledgment*) paketi ile bir SYN paketi gönderir (ACK/SYN), üçüncü aşamada ise istemci sunucuya her şeyin tamam olduğunu belirten bir onay gönderir (ACK) ve TCP bağlantısı kurulmuş olur [12].

SYN-flood yönteminde, TCP bağlantısı kurulurken, saldırganlar hedef sisteme çok fazla sayıda SYN paketi gönderir. Bu paketlerin tamamını alan hedef sistem ise, bu kaynaklar için kendi alanında bir bağlantı noktası ayırır. Ancak, gelen her SYN paketi için bağlantı alanında bir yer ayrılmasına karşın, isteklerin sonu gelmediğinden SYN/ACK paketleri gönderilemez ve sunucu bunları biriktirir, bu nedenle bahsi geçen üçlü bağlantı bir türlü tamamlanamaz ve bir noktadan sonra bu bağlantı tablosu şişer. Böylece hedef sistem yeni bağlantı alamaz ve gerçek kullanıcılarına da hizmet veremez hale gelir.

GET-Flood Saldırıları

Bu DDoS yöntemi, *HTTP* metotlarından olan *GET* ile gerçekleştirilir. Bilindiği üzere, *HTTP* de *TCP* kullanan bir protokol olup, her *HTTP* bağlantısı öncesinde muhakkak *TCP* bağlantısının kurulması gerekmektedir. Yukarıda sözünü ettiğimiz üç aşamalı *TCP* bağlantısının tamamlanmasından sonra, sunucuya *HTTP GET* isteği gönderilmektedir. *SYN-flood* yönteminde sahte kaynak *IP*ler kullanılarak, sunucuya çok sayıda *SYN* paketi gönderilmekte ve sistem bu şekilde kilitlenmekteydi. Burada ise, saldırgan taraf sunucuya istekte bulunduktan sonra, cevabı da yine kendisi almaktadır. Bu itibarla, *GET-flood* saldırılarının tek kaynaktan yapılması pratikte uygun değildir. Çok yüksek miktarda *zombi* bilgisayarın, yine yüksek miktarda yapacağı *GET* isteğiyle gerçekleştirilen bu yöntemde, sunucu bu GET isteklerini karşılayamaz ve yine gerçek kullanıcılar tarafından erişilmez hale gelir.

Land Attack

Land Attack yönteminde, saldırganlar hedef sisteme gönderdikleri paketlerin içeriğinde kaynak IP adresini, hedef IP ile aynı yaparlar. Bir başka deyişle, hedef makina kendi kendine paket gönderiyormuş gibi bir durum oluşur. Böylece, yukarıda söz ettiğimiz üç aşamalı bağlantı zincirinde, hem dışarıdan paket almış, hem de kaynak kendisi olduğundan kendisine cevap dönmüş olur. Böylece hedef sistem bir paket alması gereken birim zamanda iki paket alır ve saldırının boyutu da iki katına çıkar.

Smurf Attack

Sık kullanılan bir DDoS metodu olan *Smurf Attack* yönteminde ise, saldırgan hedef olarak belirlediği çok sayıdaki makinaya *ping* komutunu göndermektedir. Ancak saldırgan, "***IP spoofing***" yoluyla istek gönderen kaynak adreslerini, kurban makinanın IP adresi olarak değiştirir ve istek gönderilen ağdaki tüm makinalar isteğin kurban makinadan geldiğini düşünerek bu makinaya cevap dönerler. Bu durumda, çok sayıda bilgisayar bir anda kurban makinayı cevap yağmuruna tutar ve kısa bir süre içerisinde kurban bilgisayar kilitlenerek normal hizmet verememeye başlar.

Bu sayılan yöntemler dışında *ICMP Flood, UDP Flood, Slowloris* gibi saldırı türleri de, uygulamada görünen DDoS saldırısı yöntemleridir.

DDoS Saldırılarından Korunma Yöntemleri

DDoS saldırıları, günümüzde bilgisayar korsanlarının en çok tercih ettiği saldırı yöntemlerinin başında gelmektedir. Bunun en önemli sebepleri, DDoS saldırısının İnternet üzerinden kolayca bulunabilecek bazı yazılımlar ile gerçekleştirilmesi olanağı ve esas saldırganın mevcut teknoloji ile saptanmasının güçlüğü, hatta çoğu zaman imkansızlığıdır. DDoS saldırısını önlemek güçtür, zira saldırılar çok çeşitli kaynaklardan gelmekte ve *zombi*ler üzerinden yapıldığından kaynak saldırgan çoğu kez tespit edilememektedir. Ancak, DDoS saldırısını önlemeye yardımcı olacak yöntemler de vardır.

DDoS saldırısı ilk farkedildiğinde, ilk yapılması gereken, kurban konumundaki hedef sistemin saldırının geldiği IP adreslerinden gelen bağlantı isteklerini reddetmesidir. Ancak, sistemin tümden kapatılması zaten saldırganların ana amacı olduğundan, DDoS saldırısından korunurken, sistemin mümkün olduğunca açık ve çalışır vaziyette kalmasını içerecek tekniklerin kullanılması gerekmektedir.

Rate Limit adı verilen teknik, bir hedef bakımından, belli bir zaman içerisindeki trafik miktarının sınırlandırılmasıdır. Bu yöntemle normal zamandaki trafik öğrenilir ve bu trafiğe uygun bir değer limit olarak kabul edilir. Böylece kabul edilen değerin üzerindeki trafik düşürülür ve DDoS saldırısının sistemi kilitlenmesinin önüne geçilmiş olunur [13].

Çok sık uygulanmayan bir yöntem olmakla beraber *IP engellenme* de DDoS saldırılarından korunmak için kullanılan bir metottur. Hedef sistem, erişmesi gereken kaynakları belli bir aralıkta toplayabilme imkanına sahipse veya IP adresleri tek tek bilinebilecek durumdaysa, bunlar için bir liste oluşturulur ve bunlar dışındaki bütün IP'ler engellenip tüm trafik durdurularak, sisteme bilinmeyen IP'ler üzerinden saldırılmasının önüne geçilmiş olunur.

Özellikle *SYN-flood* yöntemiyle gerçekleştirilen DDoS saldırılarında kullanılan bir korunma yolu olan *SYN Proxy* yönteminde ise, *Web Proxy* mantığına benzer bir şekilde, *SYN Proxy* cihazı gerçek sunucu ile İnternet arasında durmaktadır. TCP bağlantısında anlattığımız üçlü el sıkışmadaki son ACK paketi gelmeden (üçüncü aşama), trafiğin web sunucusuna gitmesine izin vermez. Bu şekilde, tamamlanmayan *el sıkışmalar* meydana gelmez ve saldırının kurbanı olan hedef sistemin kaynakları da tüketilmemiş olur.

Saldırı sırasında kullanılan *zombi* bilgisayarların saldırıyı farkedip saldırganın önceden bilgisayarına kurduğu *daemon*'ları ortadan kaldırması da saldırıyı keseceğinden, etkili bir yoldur. Ancak DDoS saldırılarında genelde çok sayıda ve birbirinden bağımsız *zombi*ler kullanıldığından, birkaç *zombi*nin uygulayacağı bu yöntem çoğu kez saldırının şiddetini engellemekte yeterli olmamaktadır.

Bunlar dışında, uygulamada DDoS saldırılarının büyük bir kısmı *IP spoofing* yolu ile yapıldığından, *IP spoofing'i* engellemek de DDoS saldırılarından korunmanın etkili bir yoludur. Bunun için de, bilgisayar kullanıcılarının daha sıkı paket filtreleme işlemi yapan *Firewall*'lar kullanması gerekmektedir. Ancak bu yöntem, sıkı koruma tedbirleri sistemi yavaşlattığından, pek tercih edilmemektedir [14].

"Avrupa Konseyi Siber Suç Sözleşmesi" Bakımından DDoS Saldırısında Bulunan Failin Cezalandırılması

Türkiye'nin 10 Kasım 2010 tarihinde taraf olduğu "Avrupa Konseyi Siber Suç Sözleşmesi"nin 5. maddesinde, DDoS saldırısının kapsamına girdiği bir kimsenin bilişim sisteminin engellenmesi *"Sistem Engellemeleri"* başlığıyla düzenlenmiştir. Buna göre, *"Her bir taraf devlet veri yükleyerek, aktararak zarar vererek, silerek, bozarak, değiştirerek veya müdahale ederek bilgisayar sisteminin kullanımında hakkı olmadığı halde bilerek ve isteyerek bilgisayarın sisteminin çalışmasını sekteye uğratma fiilini ulusal kanununda suç olarak düzenlemeli ve gerekli diğer düzenlemeleri yapmalıdır."*

2010 yılında Sözleşmeye taraf olan Türkiye de, Sözleşmenin getirdiği yükümlülükler uyarınca, bir bilişim sisteminin işleyişini engelleme fiilini gerçekleştiren failin cezalandırılmasına ilişkin ulusal kanunlarında düzenleme yükümlülüğü altına girmiştir. Ne var ki, 2004 tarihli Sözleşmeden 1 yıl sonra yürürlüğe giren 5237 sy. TCK'nun 244. Maddesinde söz konusu eylemler suç kapsamına alınmış olduğundan, Türkiye Sözleşmeye taraf olmadan önce, 5. Maddenin gereklerini yerine getirmiştir.

DDoS Saldırısında Bulunan Failin 5237 sy. TCK Bakımından Sorumluluğu

Suçun Maddi Unsuru

DDoS saldırısında, hedef sisteme aynı anda çok sayıda bilgisayar üzerinden istek gönderildiğinden, sistem kilitlenmekte ve çalışamaz hale gelmektedir. Böylece, saldırgan esasen sistemin içine girmeksizin veya herhangi bir veriye müdahale etmeksizin, yalnızca sisteme erişilmesini engellemektedir.

5237 sayılı TCK'nun 244/1. maddesi uyarınca *"Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır."* O halde, DDoS saldırıları "*bir bilişim sisteminin işleyişinin engellenmesi*" fiiline karşılık geldiğinden, TCK m. 244'te öngörülen suça vücut vermektedir.

Aynı hükmün 3. fıkrasında ise, "*Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır*" şeklinde düzenleme yer almakta olup, DDoS saldırısının hükümde sayılan kurumların bilişim sistemleri hedef alınarak gerçekleştirilmesi halinde, bu durum kanun koyucu tarafından ağırlaştırıcı neden olarak kabul edilmiştir.

Yukarıdaki hükümler göstermektedir ki, DDoS saldırısı, TCK m. 244'te öngörülen suçun maddi unsurunu oluşturmaktadır. Zira bu hükme göre, TCK m. 244'te düzenlenen suçun meydana gelmesi için, "*bir bilişim sisteminin işleyişinin engellenmesi veya bozulması"* yeterli olacaktır. Bu itibarla, fail ister tek bir IP adresi üzerinden, isterse binlerce *zombi* bilgisayar üzerinden hedef sisteme saldırıda bulunsun, hedef sistemin işleyemez duruma gelmesi halinde TCK m. 244'ün maddi unsuru ortaya çıkmış olacaktır. Elbette, suçun mağduru olan hedef sistemin bir banka, kredi kurumu veya bir kamu kurum ve kuruluşunun bilişim sistemi olması halinde, faile verilecek ceza yarı oranında ağırlaştırılacaktır.

Suçun Manevi Unsuru

TCK'nun 21. maddesinde *"Suçun oluşması kastın varlığına bağlıdır"* dendikten sonra, 22. maddede *"Taksirle işlenen fiiller, kanunun açıkça belirttiği hallerde cezalandırılır"* hükmüne yer verilmektedir. O halde, ceza hukukunun genel ilkesi, failin kasıtlı sorumluluğu olup, bir fiilin taksirli halinden sorumlu olunabilmesi, ancak o suçun taksirli halinin ceza kanunun özel hükümler kısmında düzenlenmiş olmasına bağlıdır [15],[16].

DDoS saldırısı failinin ceza sorumluluğunun dayandığı TCK m. 244'ün taksirli hali ceza kanununda özel olarak düzenlenmediğinden, DDoS failinin manevi unsuru hiç şüphe yok ki kasıttır. Kast, TCK'nun 21/1. maddesinde *"Suçun kanuni tanımındaki unsurların bilerek ve istenerek gerçekleştirilmesi"* olarak tanımlanmıştır. Bu durumda, DDoS saldırısında bulunan kişinin cezalandırılabilmesi için, mutlaka suçu düzenleyen ceza normundaki unsurları bilerek ve isteyerek meydana getirmiş, bir başka deyişle "*hedef olarak belirlediği bilişim sisteminin işleyişini engellemek veya bozmak*" fiilini bilerek ve bu sonucu irade ederek hareket etmiş olması gerekir [17].

Bu husus, özellikle *zombi* bilgisayarların sorumluluğu bakımından büyük önem arzetmektedir. Çünkü, DDoS saldırısından dolayı ceza sorumluluğunu belirlerken failin kasıtlı hareket etmesini aramaz ve sadece somut fiilden dolayı ceza tayinine gidersek, bu durumda esasen TCK m. 244'teki maddi unsuru meydana getirmiş olan bütün *zombi* bilgisayarların kullanıcılarına TCK m. 244 uyarınca ceza vermek gerekecektir. Ancak, failin cezalandırılması için maddi unsurun yanında, ayrıca kasıtla da hareket etmiş olması gerektiğinden, saldırıdan haberi dahi olmayan ve daha öncesinde saldırgan tarafından sisteminin ele geçirilmesi suretiyle suçta araç olarak kullanılmış olan *zombi* bilgisayarların kullanıcılarının ceza sorumluluğu ortadan kalkmaktadır [18]. Aynı şekilde, örneğin bir İnternet sitesine DDoS saldırısı yapıldığı anda, bu saldırıdan habersiz bir biçimde siteye giriş yapmaya çalışarak, istemeksizin sitenin hizmet veremez hale gelmesine yardımcı olan "*gerçek kullanıcı*"ların da, manevi unsurlarının bulunmaması nedeniyle, herhangi bir ceza sorumluluğundan bahsedilemeyecektir [19].

DDoS saldırılarıyla ilgili merak edilen hususlardan birisi de, son dönemlerde sıkça gündeme gelen ve kamu kurum ve kuruluşlarının hedef alındığı protesto amaçlı yapılan DDoS saldırılarıdır. Özellikle kamuoyunda *Red Hack* ve *Anonymous* adlarıyla bilinen ve İnternet üzerinden örgütlenen kullanıcılar tarafından gerçekleştirilen protesto amaçlı DDoS eylemlerini gerçekleştiren kişilerin cezai sorumluluğunun olup olmayacağı tartışmalı bir konudur. *Red Hack* grubu tarafından gerçekleştirilen ve esasen TCK m. 243'te öngörülen "*yetkisiz erişim*" suçuna vücut veren kamu kurumlarının bilişim sistemlerinin *hacking* yoluyla ele geçirilmesi fiilleri dışında, bu iki grup ve benzeri gruplar tarafından protesto amaçlı yapılan DDoS saldırılarında ceza sorumluluğundan bahsetmek mümkün müdür?

Bilindiği üzere, yakın geçmişte bu gruplar tarafından, İnternet sansürü, kopya skandalı vb. meseleleri protesto amacıyla TİB, ÖSYM gibi kamu kurumlarının web sitelerine DDoS saldırısı yapılmış ve bu siteler belli bir süre için erişilemez hale getirilmişti. Teknik olarak bakıldığında, yapılan bu saldırılar TCK m. 244'ün maddi unsurunu oluşturduğundan ve saldırganlar hedef sistemin "*işleyişinin bozulması veya engellenmesi*" fiilini bilerek ve bu sonucu isteyerek gerçekleştirdiğinden, yapılan bu protesto eylemiyle TCK m. 244'teki suç meydana gelecek ve saldırıyı yapanların TCK m. 244/3 uyarınca

cezalandırılmasının şartları oluşacaktır.

Ne var ki, kanaatimizce, protesto amacıyla yapılan DDoS saldırıları ile salt bir kişi veya kuruma zarar vermek amacı taşıyan saldırıların birbirinden ayrılması gerekmektedir. Ceza hukukunda failin saikinin manevi unsurun oluşması bakımından bir etkisi olmamakla ve falin "*esas niyeti*"nden bağımsız olarak ceza normunda öngörülen fiilin unsurlarının bilerek ve isteyerek gerçekleştirilmesinin suçun oluşması için yeterli olmasıyla birlikte; protesto amacıyla yapılan fiillerde durum farklılaşabilmektedir. Örneğin, kamuya açık bir alanda birden çok kişinin bir araya gelerek bağırıp çağırması TCK m. 123'te düzenlenen *"Kişilerin Huzur ve Sükununu Bozma"* suçuna vücut verebilecekken, bir protesto gösterisi yapan binlerce kişinin şehrin en işlek meydanlarında "*gürültü*" yapması, Anayasal bir hakkın kullanılması olduğundan, ilgili suça sebebiyet vermeyecektir. Benzer biçimde, protesto amacıyla yapılan DDoS saldırılarında da fail ya da failler gerçekleştirdikleri fiilin ceza normunda öngörülen suçun kurucu unsurlarına vücut verdiğini bilmekte ve istemekteyseler de, somut olayda yargıcın faillerin kasıtlarının saldırı yapılan kurumun bilişim sisteminin işleyişinin bozulması olmadığı ve Anayasa ve Avrupa İnsan Hakları Mahkemesi kararları uyarınca "*protesto hakları*"nı kullandıkları yorumunu yapması halinde, faillere manevi unsur yokluğundan ceza verilmemesi mümkün hale gelebilecektir. Zira Ceza Muhakemesi Kanunu uyarınca yargıç, gerekçesini belirtmek üzere, vicdani kanaatine göre hüküm tesis eder [20]. Bu bağlamda, yargıç somut olay koşullarına göre yapılan "*protesto eylemi*"nin ifade özgürlüğünün bir uzantısı olduğuna kanaat getirir ve faillerin TCK m. 244'teki fiil bakımından manevi unsur taşımadıkları sonucuna varırsa, protesto amaçlı DDoS saldırısı için ceza vermeyebilecektir. Ancak, tekrar etmek gerekir ki, hangi saikle yapılırsa yapılsın, bilerek ve isteyerek yapılan DDoS saldırısı TCK m. 244'te öngörülen suçun oluşması için yeterlidir.

SONUÇ

DDoS saldırısı, gerek saldırganın saptanmasının neredeyse imkansız olması, gerekse gelişen teknoloji ile beraber işlenmesinin kolaylığı ve işlenme yönteminin çokluğu bakımından, son dönemlerde en çok tercih edilen bilişim suçlarının başında gelmektedir. Failin bilişim sisteminin içerisine girmediği, yalnızca daha önceden ele geçirmiş olduğu çok sayıdaki *zombi* bilgisayar yoluyla, hedef olarak belirlediği bir bilişim sistemine aynı anda çok miktarda istek göndererek, hedef sistemi erişilemez hale getirdiği DDoS saldırısının, *"bir bilişim sisteminin işleyişinin engellenmesi"* olarak düzenlenen TCK m. 244 uyarınca suç olduğu tartışmaya yer vermeyecek biçimde açıktır.

DDoS saldırısında saldırgan, teknik olarak saldırının içerisinde yer almadığından ve tespit yapıldığında suç işlendiğinden tamamen habersiz olan *zombi* bilgisayarların IP adreslerine ulaşıldığından, şüphelenilen bir kişinin bulunmaması halinde, suç işlendikten sonra failin tespit edilmesi neredeyse imkansızdır. Zira, uygulamada ancak saldırı yaptığından şüphelenilen kişilerin bilgisayarlarına CMK m. 134 uyarınca el konulduğunda ve bilgisayarların *harddisk*lerinde inceleme yapıldığında, DDoS saldırısının yapıldığına dair teknik delil elde edilmesi mümkün olup, bunun haricinde hedef sistem veya *zombi* bilgisayarların IP adresleri üzerinden esas saldırgana ulaşmak mümkün olmamaktadır. Bu itibarla, DDoS saldırısına karşı alınacak önlemler de, ancak saldırı yapılmadan önce alınacak tedbirler ve güvenli İnternet kullanımıyla mümkün olabilmektedir. DDoS saldırılarının yoğunluğu ve etkilerinin yüksek olması, çok sayıda *zombi* bilgisayar kullanılması ile ilgilidir. O yüzden, günümüzde özellikle sermayeleri bilişim sistemleri olan firmaların (yazılım şirketleri, *hosting* firmaları vs.) bu saldırılardan mağdur olduğu ve uzun süreli ve şiddetli DDoS saldırıları sonucu birçok bilişim firmasının ticari faaliyetlerini sonlandırmak zorunda kaldığı düşünüldüğünde, çağımızın popüler suç tipi DDoS saldırılarının önünün kesilmesi büyük önem arzetmektedir. Nitekim, *hosting* firmalarının saldırıya uğraması, onlardan hizmet alanların ve dolayısıyla son tahlilde bireysel İnternet kullanıcılarının da güvenliklerinin tehdit altında olduğunu göstermektedir. Bu saldırıları engellemenin ilk yolu, yukarıda sözünü ettiğimiz üzere, *zombi* olmamaktan ve güvenli İnternet kullanmaktan geçmektedir. Kullanılan bilgisayarlara kısa periyodlarla yeni güvenlik yamalarının kurulması ve son sürüm yazılımlar kullanılarak bilgisayarlara yerleştirilmesi olası DDoS *daemonlar*ının tespiti, *zombi* olmamak için atılacak ilk adımlardandır. *Zombi* sayısı azaldığı ölçüde, kendisine suç aracı bulamayacak olan DDoS saldırganlarının da önü kesilecek ve bilgi toplumunun büyük vebası bilişim suçlarıyla mücadelede önemli bir eşik aşılmış olacaktır.

KAYNAKÇA

[1] KETİZMEN, Muammer; Türk Ceza Hukukunda Bilişim Suçları, Ankara, 2008.

[2] ÖZEN, Muharrem / BAŞTÜRK, İhsan; Bilişim – İnternet ve Ceza Hukuku, Ankara, 2011.

[3] http://www.pclabs.com.tr/2011/06/09/dos-ya-da-ddos-saldirisi-nedir/ (20.09.2012).

[4] http://www.teknoturk.org/docking/yazilar/tt000002-yazi.htm (20.09.2012).

[5] http://ddos-nedir.blogspot.com (20.09.2012).

[6] AHİ, Gökhan; Anonymous ve Siber Ataklara Hukuksal Bir Yaklaşım, http://www.bilisimhukuk.com/2011/06/anonymous-ve-siber-ataklara-hukuksal-bir-yaklasim/, (20.09.2012).

[7] ALTUNDAL, Ömer Faruk; DDoS Nedir, Ne Değildir, http://www.siberguvenlik.org.tr/ddos-nedir-ne-degildir-bolum-2/, (20.09.2012),

[8] ALTUNDAL, a.g.e. (20.09.2012),

[9] ALTUNDAL, a.g.e. (20.09.2012),

[10] ALTUNDAL, a.g.e. (20.09.2012),

[11] http://www.bilisimterimleri.com/bilgisayar_bilgisi/bilgi/ 55.html (30.10.2012),

[12] http://www.webmastersitesi.com/webmaster-sozlugu/22725-syn-flood-nedir.htm (21.09.2012),

[13] http://en.wikipedia.org/wiki/Rate_limiting (21.09.2012).

[14] ALTUNDAL, a.g.e. (20.09.2012),

[15] TOROSLU, Nevzat; Ceza Hukuku Genel Kısım, Ankara, 2011.

[16] CENTEL, Nur /ZAFER, Hamide / ÇAKMUT, Özlem; Türk Ceza Hukukuna Giriş, İstanbul, 2006.

[17] SINAR, Hasan; İnternet ve Ceza Hukuku, İstnabul, 2001.

[18] KURT, Levent; Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Ankara, 2005.

[19] ÖZDİLEK, Ali Osman; Uygulamadan Örnek Olaylarla Bilişim Suçları ve Hukuku, İstanbul, 2006.

[20] FEYZİOĞLU, Metin; Ceza Muhakemesinde Vicdani Kanaat, Ankara, 2002.