LÖDDOS

DDoS Saldırıları Değerlendirme Raporu

LoDDOS

İÇİNDEKİLER

DDoS : Distributed Denial of Service
IoT : Internet of Things
TCP : Transmission Control Protocol
UDP : User Datagram Protocol
NTP : Network Time Protocol
SSDP : Simple Service Discovery Protocol
SMTP : Simple Mail Transfer Protocol
OSI : Open Systems Interconnection
CDN : Content Delivery Network
Gbps : Giga bit per second
PPS : Packet Per Second
WAF : Web Application Firewall
IPS : Intrusion Prevention System
DNS : Domain Name System

KISALTMALAR

YÖNETİCİ ÖZETİ

DDoS saldırıları gün geçtikçe karmaşıklaşmakla birlikte, DDoS saldırısı düzenlemek çok kolay ve düşük maliyetli olmaktadır. Saldırganlar çok düşük ücretler karşılığında, sadece hedef adresi girerek DDoS saldırısı gerçekleştirebilmekte ve organizasyon sistemlerini işlevsiz hale getirebilmektedir. DDoS saldırılarının bu kadar kolay ve ucuz maliyetlerle gerçekleştirilebilmesi internet üzerinden işlerini yürüten organizasyonlar için büyük bir risk oluşturmaktadır. Bu tip DDoS saldırılarına hazırlıksız yakalanan organizasyonlar saatler ve hatta belki günler boyunca hizmet veremez duruma gelebilmektedir.

DDoS saldırıları internet üzerinden hizmet veren tüm organizasyonlar için risk oluşturmaktadır. Bu tip saldırılara karşı gerekli hazırlıkların yapılması, teknik ve idari tedbirlerin alınması ve sistemlerin DDoS dayanıklılığının sürekli olarak test edilerek savunma mekanizmalarının iyileştirilmesi önemlidir.

Bu rapor dahilinde; DDoS, DDoS çeşitleri, DDoS saldırılarının arkasındaki motivasyonlar, tarihte yaşanmış büyük DDoS olayları, DDoS saldırılarından korunma yaklaşımı ve DDoS testlerinin önemli üst seviyede açıklanmıştır.

DoS/DDoS Saldırısı Nedir?

"**Distributed Denial of Service (DDoS)**" Saldırısı kavramını tanımlamadan önce **Denial of Service (DoS)** Saldırısını tanımlamak daha uygun olacaktır. **DoS saldırısı,** hedef bir sistemi meşru kullanıcıları tarafından kullanılamaz hale getirmeyi hedefleyen bir saldırı çeşididir. Bu saldırılar hedef sistem ve uygulamaları veya bu sistem ve uygulamalara erişimde kullanılan diğer kaynakları sömürme yöntemini kullanarak, hedeflerin işlevsiz hale getirilmesini amaçlar. **DDoS** ise saldırganların bu saldırıları gerçekleştirirken, dağıtık yapıdaki çok sayıda saldırı kaynağını aynı amaç doğrultusunda kullanmasıdır. Çok fazla sayıda ve çeşitli tipteki (bilgisayar, mobil cihaz, IoT vb.) saldırı kaynağı kullanılması ile hem saldırıların kolaylıkla engellenmesinin önüne geçilmesi hem de hedef sisteminin kaynaklarının daha hızlı ve kolay şekilde sömürülmesi hedeflenir. Saldırganlar genellikle internete açık bilgi işlem kaynaklarını zararlı yazılım bulaştırma yoluyla ele geçirip (zombie/bot), bu cihazları toplu olarak (botnet) kontrol edebilen mekanizmalar sayesinde (Command and Control/C2/C&C) hedefledikleri sistemlerin kaynaklarını tüketme niyetiyle kullanma yöntemini tercih etmektedir.

DDoS Saldırı Çeşitleri

Saldırganlar genel olarak üç tip DDoS saldırı (Ağ, Protokol ve Uygulama) yöntemi kullanmaktadır.

Bu saldırı tipleri aşağıdaki başlıklarda tanımlanmıştır.

Volümetrik Saldırılar

Protokol Saldırıları

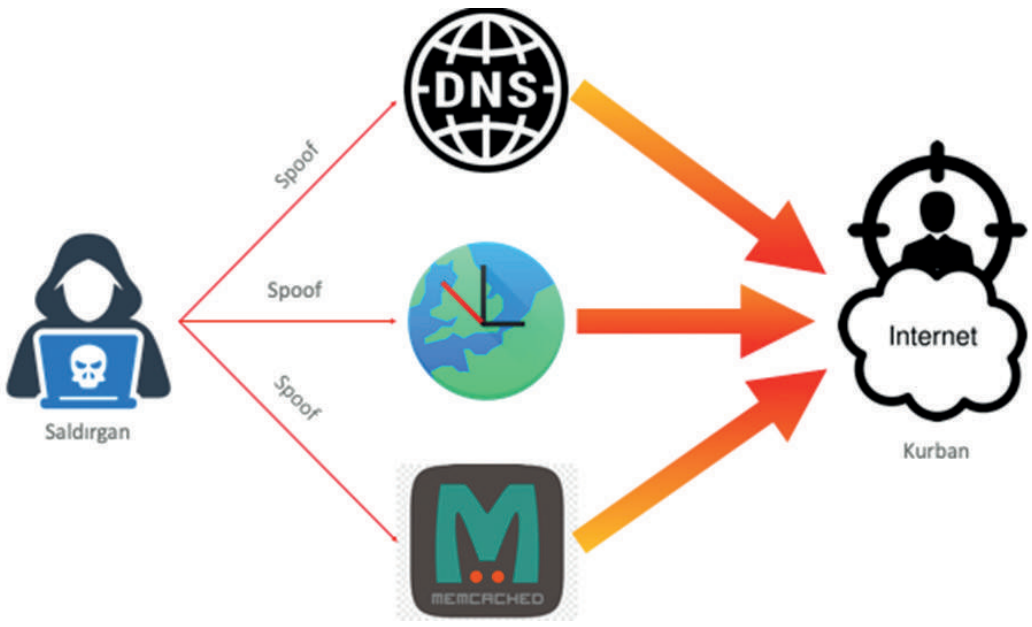
Uygulama Saldırıları

Volümetrik Saldırılar (Ağ)

Saldırganlar tarafından en sık kullanılan atak çeşidi olup hedef organizasyonların kullanmakta olduğu internet bant genişliğini tüketmeyi hedeflemektedir. Bu şekilde gerek organizasyona gelen ağ trafiği gerek organizasyondan dışarı çıkan ağ trafiği etkilenecek ve meşru isteklere cevap veremeyerek servis dışı kalacaktır. Sonuç olarak internet altyapısını kullanan tüm taraflar etkilenecek ve internet bağımlı tüm hizmetler işlevsiz kalacaktır.

Volümetrik saldırılara örnek olarak; TCP/UDP Flood, DNS/NTP/Mamcached Amplifikasyonu saldırıları verilebilir.

Amplifikasyon Saldırıları: Saldırganların internette genel kitlelere hizmet vermekte olan sunuculardaki DNS, NTP, SSDP, memcached vb. protokolleri kullanarak yaptıkları saldırılardır. Kurban (hedef) sistemlere saldırırken, sanki kurban sistemlerden istekte bulunuyormuş gibi yapıp (spoof), geri dönüş paketlerinin kurban sisteme ulaşmasını sağlayarak DDoS gerçekleştirirler. Bu saldırıda güvenli olarak yapılandırılmamış sunuculara küçük boyutlarda istek paketleri gönderilir, kurban sisteme büyük boyutlarda paket gönderilmesi sağlanır. Kurban sistemler büyük boyutlu ve çok sayıdaki isteğe yanıt veremez duruma gelince işlevsiz kalır.



Şekil 2

Protokol Saldırıları

Genel olarak OSI L3/L4 protokollerini hedef alan saldırılardır. Genellikle bağlantı oturum bilgisi (session) kullanan Güvenlik Duvarı, Yük Dengeleme Cihazları, Yönlendiriciler vb. sistemleri hedef alınır. Çok sayıda oturum açma isteğinde bulunup, oturum tamamlanmadan yeni istekler gönderilir. Bu şekilde ağ ve güvenlik cihazlarının oturum tablolarını doldurup işlevsiz hale gelmesi sağlanır. Protokol saldırılarına örnek olarak SYN/SYN-ACK/ACK Flood, Ping of Death vb. verilebilir.

Uygulama Saldırıları

Web uygulamaları, DNS, SMTP vb. OSI L7 uygulama servislerine yapılan ataklardır. Hedef uygulamalara kapasitelerinin çok üzerinde istek gönderilerek, kaynaklarının tüketilmesi yöntemi ile sistemin işlevsiz hale getirilmesi asıl amaçtır.
Uygulama saldırılarına örnek olarak HTTP, HTTPS, DNS ve SMTP servislerine yapılan Flood atakları verilebilir.

Yukarıda bahsedilen ataklar saldırganlar tarafından teker teker yapılabileceği gibi birden fazla saldırı tipi (multi-vector) aynı anda da gerçekleştirilebilir. Bu şekilde saldırganlar, saldırılarını daha kompleks hale getirerek hem olay müdahale ekiplerinin hem de güvenlik cihazlarının engellemeye yönelik çalışmalarını zorlaştırmayı hedeflerler.

Saldırı Motivasyonları

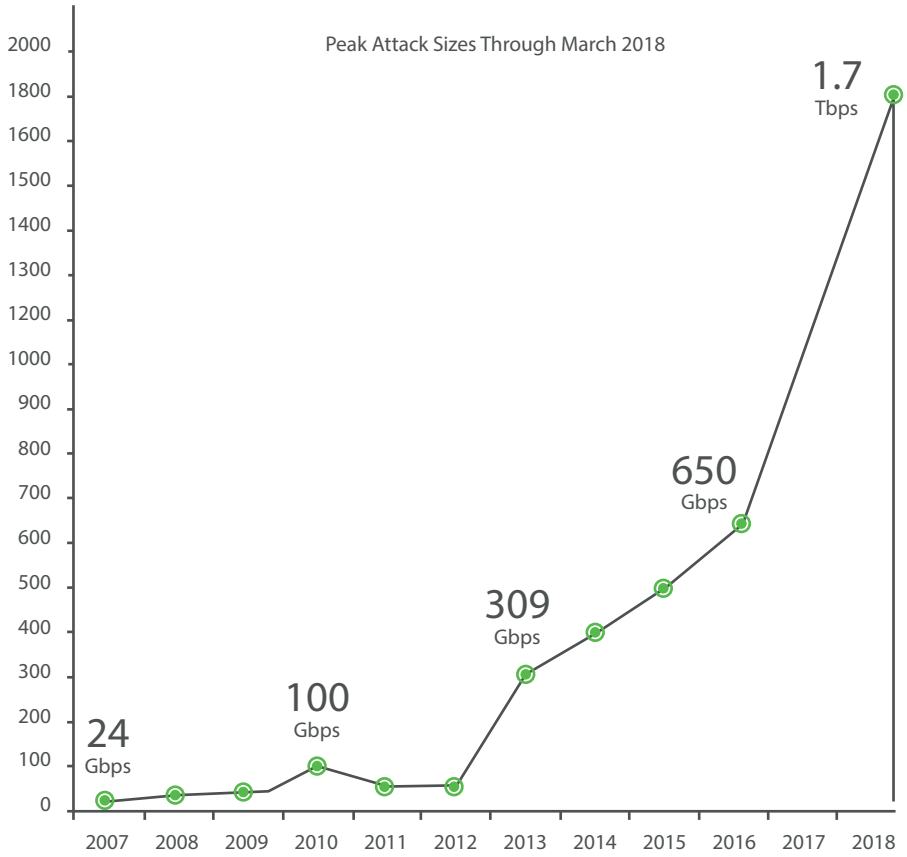
DDoS saldırılarının arkasında birçok motivasyon faktörünün olması mümkündür. Bunlardan birkaç tanesine değinmeye çalışırsak;
Para: Sonucu para kazanma veya para kaybettirmeye yönelik gerçekleştirilen ataklara tekabül eden motivasyondur. Rakip firmalara karşı avantaj sağlama çabası, şantaj yoluyla para alma, hisse değeri kaybettirme vb. sebeplerden dolayı olabilir.
İdeolojik: Siyasi, politik vb. nedenlerden ötürü gerçekleştirilir.
Saldırı Gizleme: Hedef organizasyonun personel ve cihazlarını oyalayarak asıl niyet olan veri sızdırma vb. faaliyetlerin tespitini engellemeye yönelik olarak gerçekleştirilir.
Bunlar genel olarak bahsi geçen motivasyonlar olup ek olarak farklı motivasyonların da olması söz konusudur.

Yaşanmış Olaylar

Her geçen gün birçok organizasyon DDoS saldırılarına maruz kalmaktadır. Bu başlıkta, bu saldırıların yapıldığı tarihte önem arz etme durumuna göre birkaçından bahsedilecektir.

Hizmet Sağlayıcı (İsmi Açıklanmayan): 1.7 Tbps / 2018

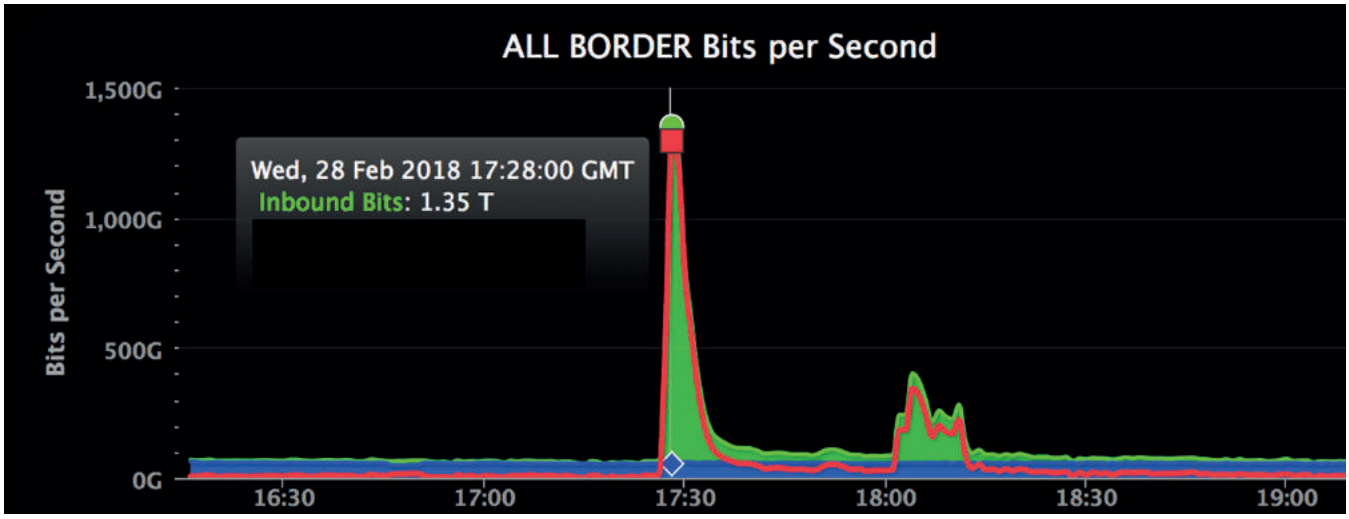
Netscout, 5 Mart 2018 tarihinde şimdiye kadar yapılan en büyük boyuttaki DDoS saldırısının gerçekleştirildiği açıklanmıştır. 1.7 Tbps boyutundaki bu saldırı Memcached Amplifikasyon tipinde olup ABD menşeli bir hizmet sağlayıcıya yapılmıştır. Yapılan açıklamalara göre bu saldırı bertaraf edilebilmiştir.



Şekil 3

GitHub: 1.3 Tbps / 2018

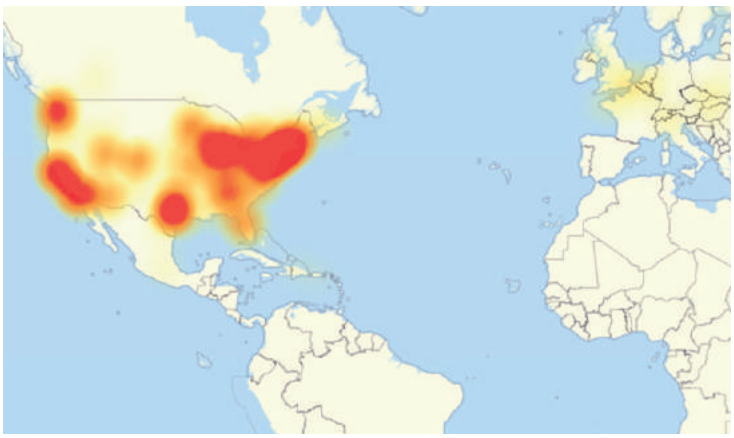
Yazılım geliştiricilerin geliştirdikleri uygulamaları depoladığı ve paylaştığı bir platform olan GitHub, 2018 senesinde 1.35 Tbps boyutunda bir DDoS saldırısına maruz kalmıştır. Yaklaşık 10 dakika boyunca siteye erişimde kesintiler yaşanmış, sonrasında servis sağlayıcının DDoS koruma hizmetinin devreye girmesiyle saldırı bertaraf edilmeye başlanmıştır. Bu atakta saldırganlar Memcached amplifikasyonu tipindeki saldırı yöntemini kullanmışlardır.



Şekil 4

Dyn: 1.2 Tbps / 2016

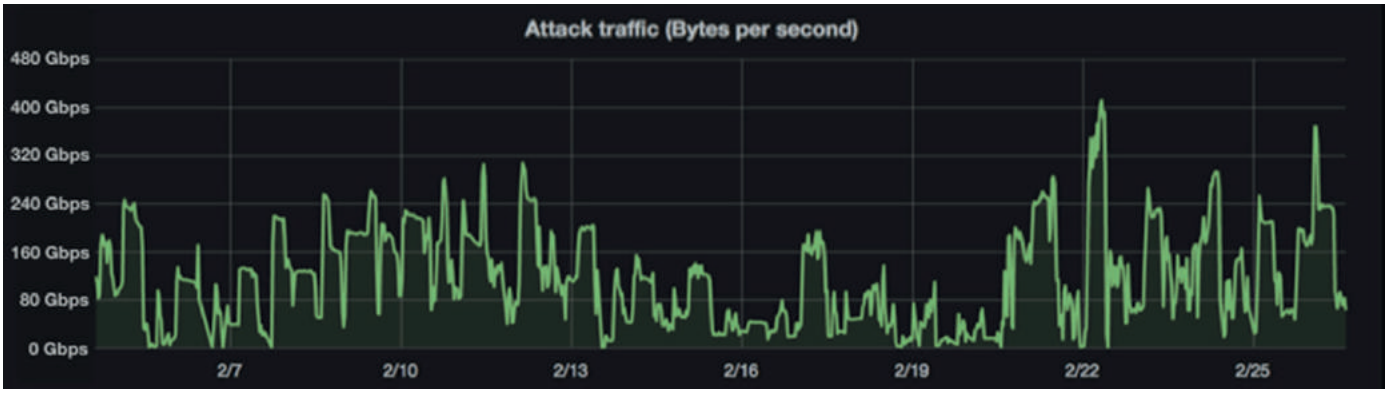
21 Ekim 2016 tarihinde DNS servis sağlayıcısı olan Dyn firmasına 1 Tbps boyutunda çeşitli zaman aralıklarıyla DDoS saldırıları gerçekleştirilmiştir. Bu saldırılarda IoT cihazlarından oluşan Mirai botnet kullanılmış ve 53 numaralı port üzerinden TCP ve UDP trafiği ile saldırılmıştır. İlk atağın durdurulması yaklaşık 2,5 saat sürmüş ancak sonrasında yeni ataklarla karşılaşılmıştır. Ataklar sırasında birçok internet sitesine erişimde sıkıntılar yaşanmıştır.



Şekil 5

CloudFlare: 400 Gbps / 2014

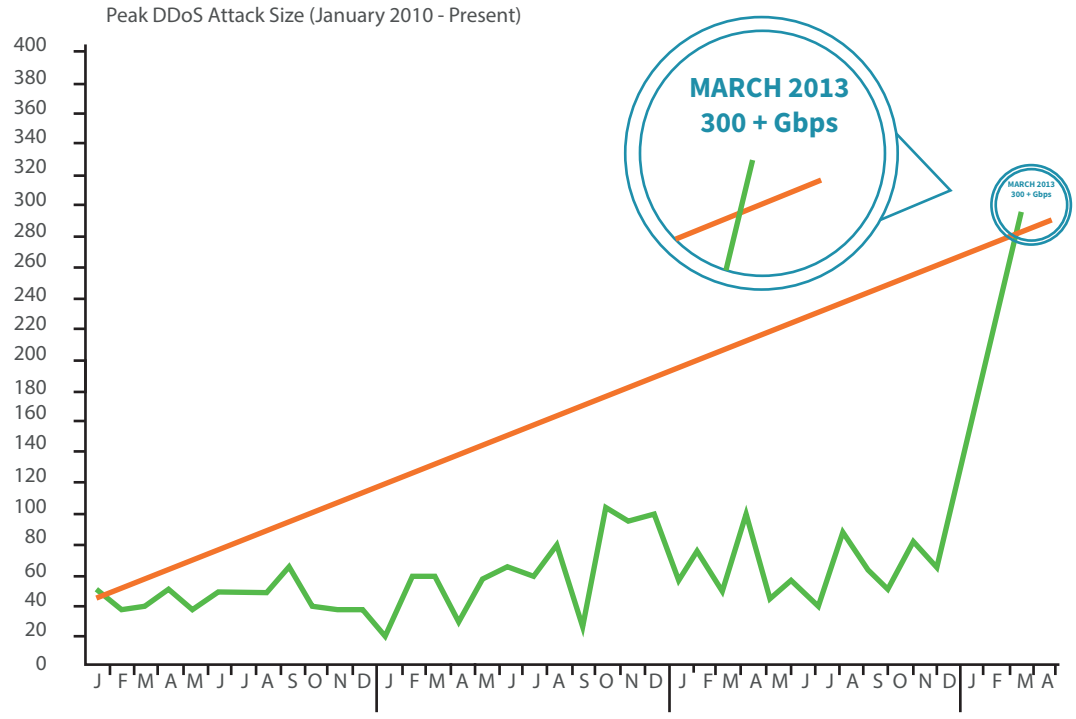
CloudFlare bir Content Delivery Network (CDN) hizmet sağlayıcısıdır. 2014 yılında CloudFlare üzerinde hizmet veren bir organizasyona 400 Gbps boyutunda bir saldırı yapılmış ve bu saldırı CloudFlare'in kendi sistemlerini bile etkilemiştir. Bu saldırıda, sunucuların saat senkronizasyonu yapmasına olanak sağlayan Network Time Protocol (NTP) kullanılmıştır



Şekil 6

SpamHaus: 300 Gbps / 2013

2013 yılında, spam e-postalarla mücadele eden SpamHaus organizasyonuna 300 Gbps boyutunda bir DDoS saldırısı gerçekleştirilmiştir. O zamana kadar gerçekleştirilmiş en büyük boyuttaki bu atak servis SpamHaus'un hizmet aldığı servis sağlayıcı tarafından durdurulmuştur.



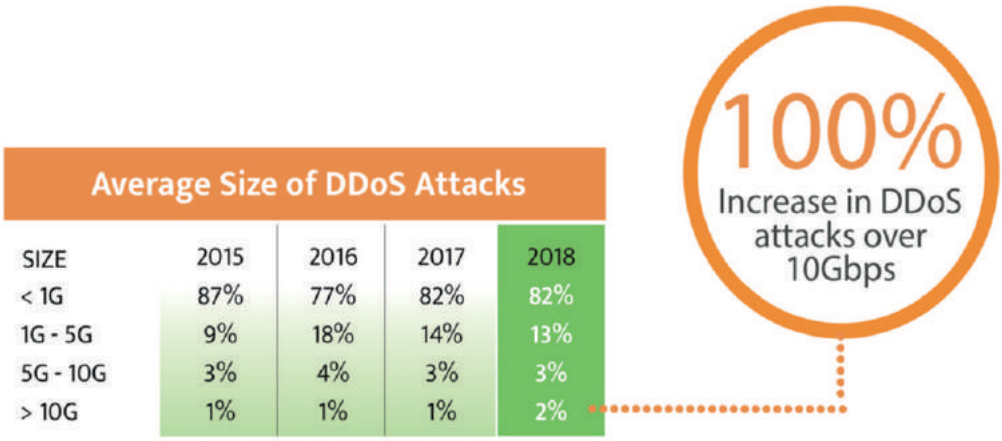
Şekil 7

Yukarıdaki olaylardan görüldüğü üzere güvenlik hizmeti sağlayan servis sağlayıcılar bile büyük boyutlu DDoS saldırılarından etkilenebilmektedir. Yukarıda açıklanmaya çalışılan atak boyutları çok büyük olup bu boyutlardaki saldırılara nadir rastlanmaktadır.

Çeşitli İstatistikler

DDoS saldırıları ile ilgili olarak yayınlanan bir takım global raporlardan elde edilen istatistikler, genel olarak DDoS saldırılarının profillenmesi açısından faydalı olacaktır.

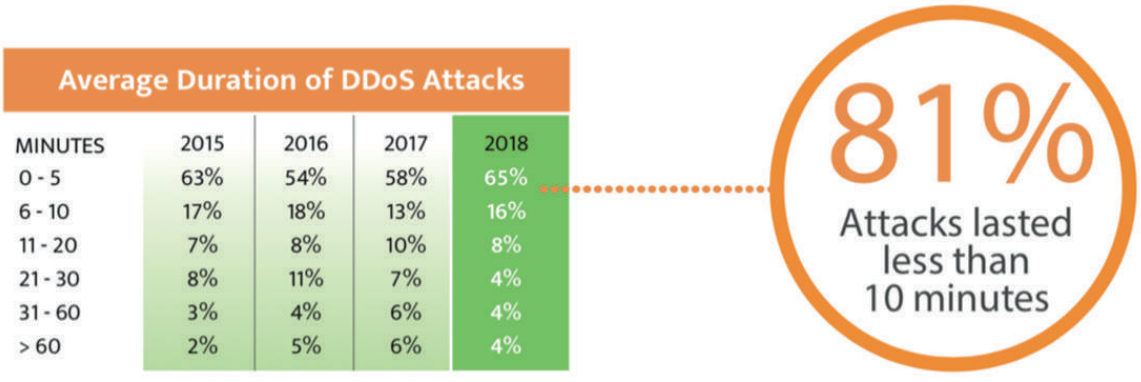
2018 Corero Trends Raporunda yer alan iki grafiği ele almak gerekirse:



Şekil 8

Yukarıdaki grafiğe göre:

- 2018 yılında gerçekleştirilmiş olan DDoS ataklarının %82'si 1 Gbps veya daha düşük boyutta olmuştur.
- 1 Gbps ile 10 Gbps arasında gerçekleştirilen atakların oranı %16
- 10 Gbps'den daha büyük boyutlarda gerçekleştirilen atakların oranı ise toplam atakların %2'sidir.
- Bu oran 2017 yılına göre %100 bir artışa tekabül etmektedir.

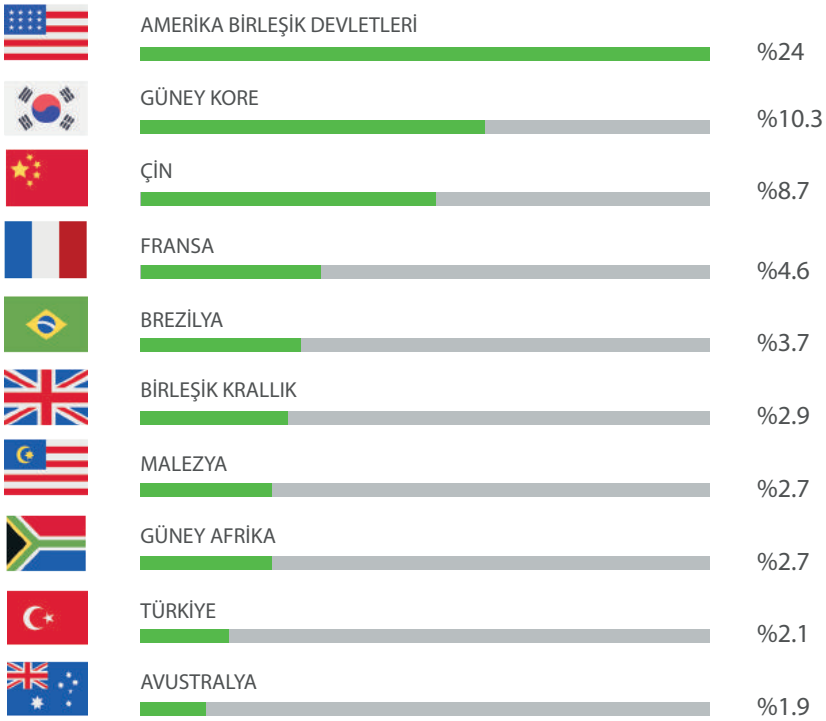


Şekil 9

Yine 2018 Corero Trends Raporunda yer alan önemli bir grafik yukarıda yer almaktadır. Bu grafiğe göre:

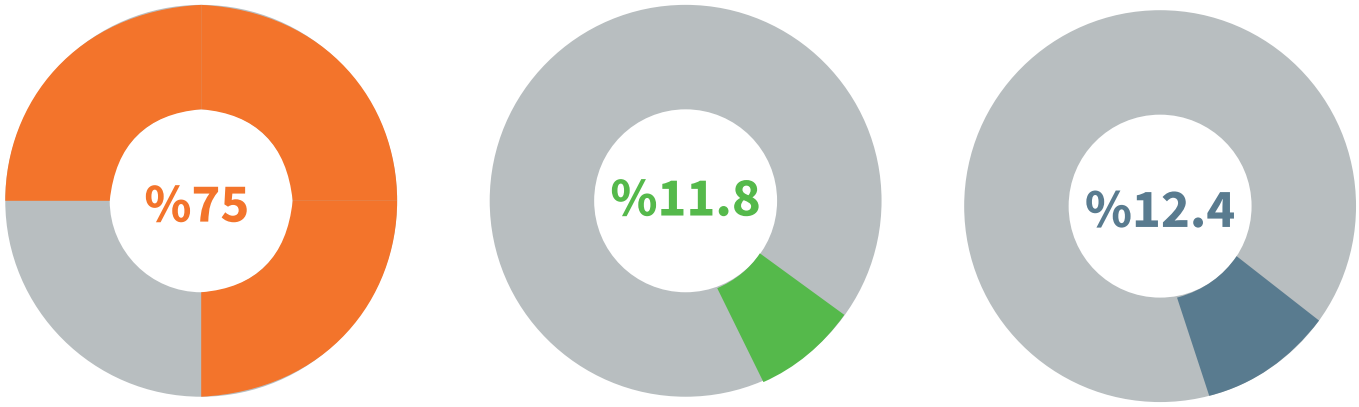
- 2018 yılında gerçekleştirilen atakların %81'i 10 dakika veya daha az sürmüştür.
- Gerçekleştirilen DDoS saldırılarının %96'sı 60 dakika veya daha az süreli olmuştur.

Figure AT11 Top Targeted Countries for DDoS Attacks by Percentage



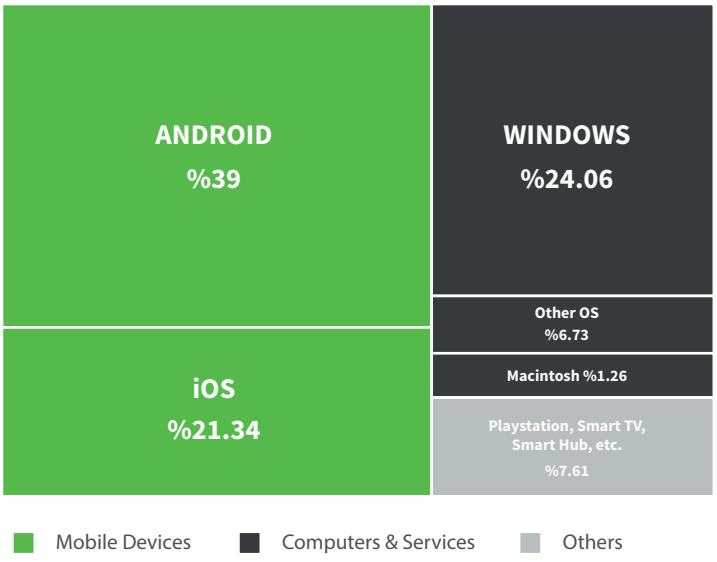
Şekil 10

Q4 2017 Global DDoS Threat Landscape Raporuna göre DDoS atağı gerçekleştirilen ülkelerin başında ABD, Güney Kore ve Çin yer almaktadır. Ayrıca %2.1'lik oran ile Türkiye de en çok atak gerçekleştirilen ülkeler arasında yer almaktadır.



Şekil 11

2018 yılında yayınlanan NETSCOUT Threat Intelligence Raporuna göre gerçekleştirilen DDoS saldırılarının %75.7'si volümetrik tiptedir. %12.4 uygulama katmanı, %11.8 protokol ataklarıdır.



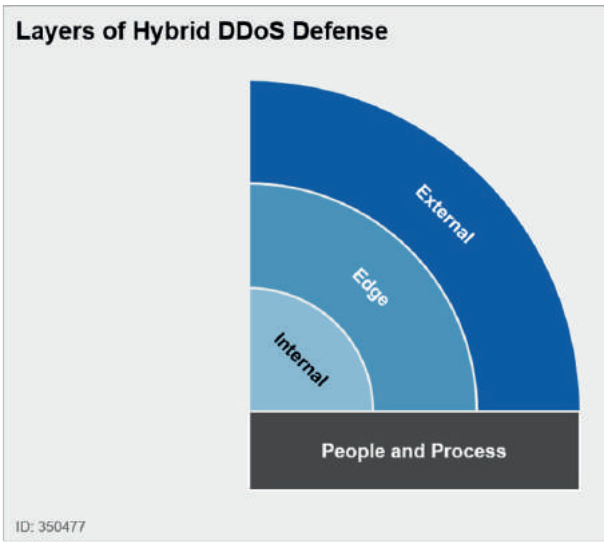
Şekil 12

Cep telefonu kullanımının artması, cep telefonlarının sahip olduğu işlemci ve belleklerin boyutlarının büyümesi ve bu cihazların **7/24** açık olması, bu cihazların saldırganlar tarafından aktif olarak DDoS saldırılarında kullanılması durumunu ortaya çıkarmıştır. Yukarıdaki grafikte son dönemlerde yaşanan DDoS olaylarının yaklaşık %60'ında botnet üyesi olarak mobil cihaz kullanımı olduğu görülmektedir.

Korunma Yaklaşımı

Yukarıdaki başlıklarda da anlatılmaya çalışıldığı üzere DDoS saldırıları çeşitli türlerde ve boyutlarda olabilmektedir. Tüm DDoS saldırı türlerini durdurabilecek tek bir cihaz veya yöntem ne yazık ki bulunmamaktadır. DDoS saldırılarına karşı dirençli olabilmenin yolu, tıpkı diğer güvenlik çalışmalarında da olduğu gibi katmanlı bir savunma mekanizması oluşturmaktan geçmektedir.

Bu savunma mekanizmasının nasıl olması gerektiği konusunda Gartner, "DDoS: A Comparison of Defense Approaches" adlı raporunda aşağıdaki şekildeki gibi birçok savunma katmanından oluşan bir tespit ve önleme yöntemi önermektedir.



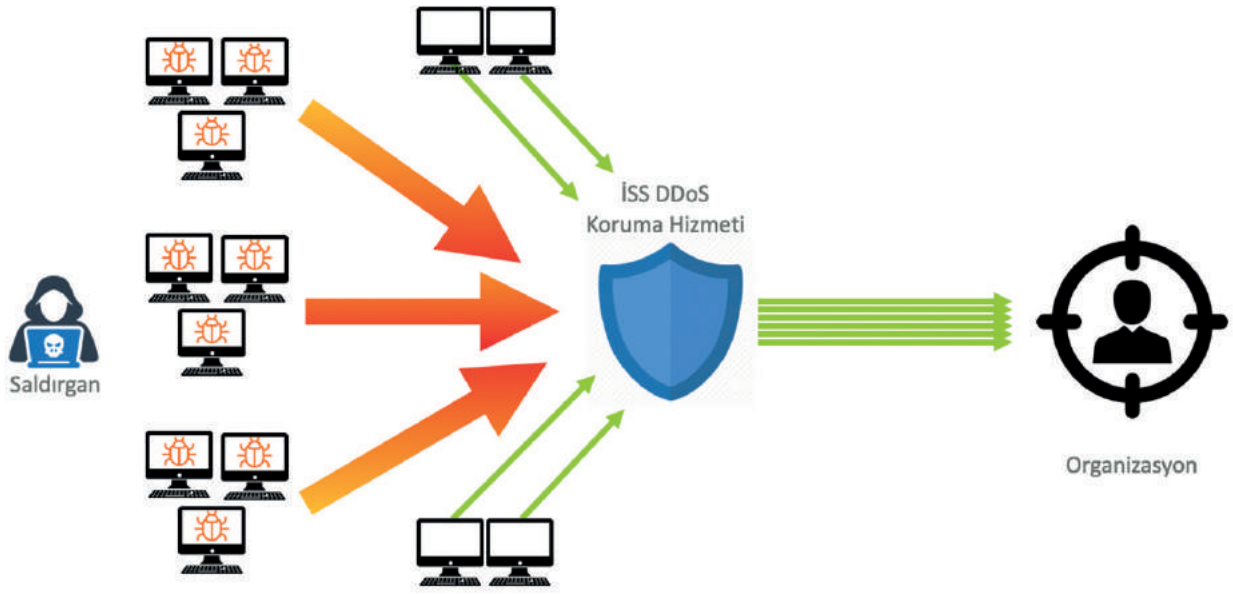
Şekil 13

Bu katmanlara değinmek gerekirse;

Dış Katman (External)

Volümetrik atakların detaylarından yukarıda bahsetmiştik. Yüksek boyutlardaki volümetrik ataklar organizasyon ağına ulaşabilirse, ne yazık ki böyle bir durumda organizasyonların güvenlik tedbirleri saldırıyı engelleme noktasında yeterli olmayacaktır. Bu ataklar organizasyon ağına ulaşmadan, engellemeye veya etkilerini azaltmaya yönelik çalışmalar gerçekleştirilmelidir. Bu noktada İnternet Servis Sağlayıcılar (İSS) ve İSS'lerin sağladığı DDoS Koruma Hizmetleri devreye girmektedir. Çok yüksek boyutlarda trafikleri işleyebilen İSS'ler, zararlı trafik organizasyon ağına ulaştıktan kısa bir süre sonra (İSS'ye göre bu süre değişiklik gösterebilmektedir) devreye girip DDoS saldırısının etkilerini azaltabilmektedir.

Bu açıdan bakıldığında organizasyonların iş gereksinimlerine uygun boyutlarda bir DDoS Koruma Hizmeti almaları önem arz etmektedir.



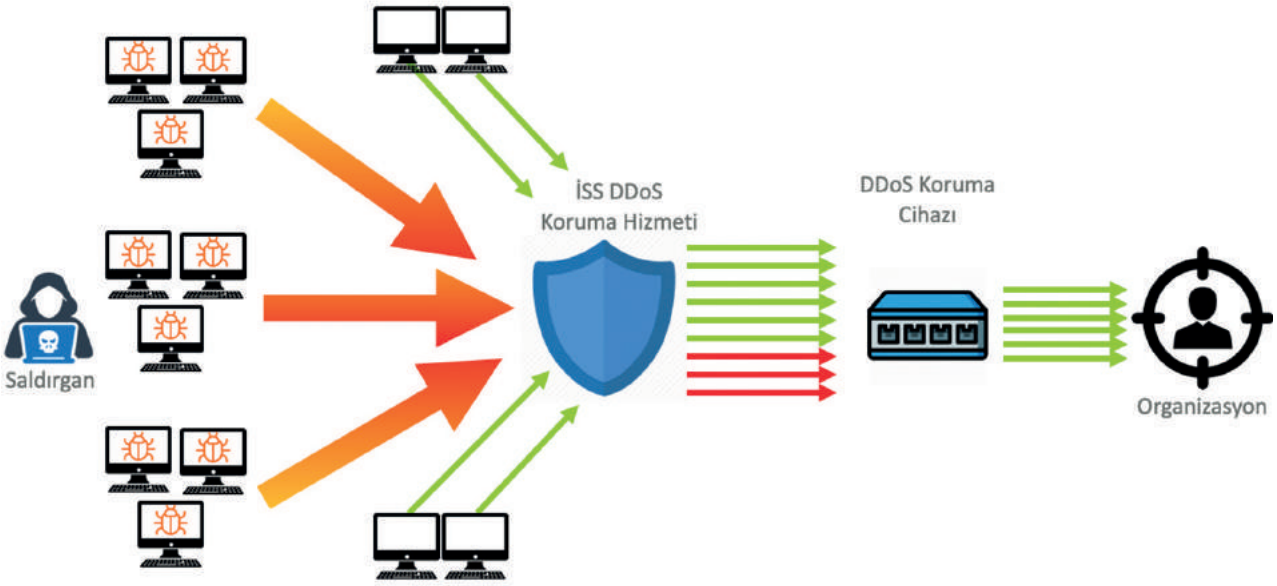
Şekil 14

Sınır Katman (Edge)

Organizasyonlara ait IP yönlendirici (router), yük dengeleyici, güvenlik duvarı ve benzeri kenar ağ ve güvenlik cihazlarının bulunduğu katmandır. Saldırganlar protokol saldırıları (TCP-SYN vb.) ile bu cihazların oturum tablolarını tüketerek IP yönlendirici, yük dengeleyici, güvenlik duvarı vb. cihazların işlevsiz kalmasını sağlayabilirler.

Bu ağ ve güvenlik cihazlarının korunmasına yönelik olarak geliştirilmiş DDoS Koruma Cihazları siber güvenlik pazarında mevcuttur. Bu cihazlar oturum (session) bazlı çalışan ağ ve güvenlik cihazlarına karşı gerçekleştirilen DDoS saldırılarının engellenmesine yönelik olarak geliştirilmiş teknolojilerdir.

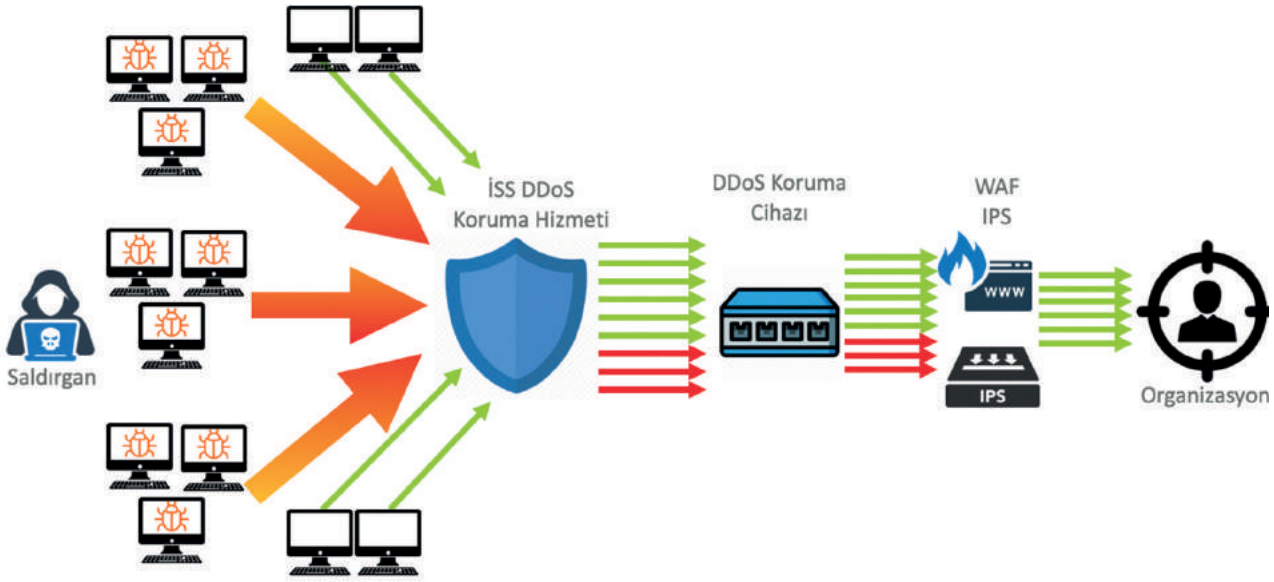
Sınır katmanında bulunan organizasyon sistemlerinin korunması açısından bu cihazların, organizasyonun internete en yakın dış noktasına konumlandırılması önem arz etmektedir. Hatta bazı DDoS koruma cihazları, İSS'de yer alan ve DDoS koruma hizmetini sağlayan cihazlar ile sinyalleşme sağlayarak daha etkin bir DDoS koruma mekanizması sağlamaktadır.



Şekil 15

İç Katman (Internal)

Ağ, protokol ve uygulama tiplerindeki DDoS saldırılarından belki de en tehlikelisi uygulama seviyesinde gerçekleştirilen ataklarıdır. Genellikle doğrudan kullanıcıya hizmet veren web, e-posta, DNS vb. uygulamalara yönelik olarak gerçekleştirilir ve ilgili uygulamanın işlevsiz kalmasını sağlarlar. Özellikle DNS atağı başarılı olursa DNS bağımlı tüm uygulamalar erişilemez olacaktır. İnternete açık uygulamaların korunmasına yönelik olarak IPS, WAF vb. cihazlar kullanılmaktadır. Bu cihazlar uygulamaların yapılarını keşfederek uygulamaya özel koruma mekanizmalarını devreye alabilecek yeteneğe sahiptir.



Şekil 16

İnsan ve Süreç (People and Process)

En kaliteli DDoS koruma hizmet ve cihazları (Teknoloji) alınmış olsa da etkin bir siber savunma için **İnsan-Süreç-Teknoloji** unsurlarının tümünün uyumlu bir şekilde kullanılması gerekmektedir. Bu noktada İnsan ve Süreç unsurlarının DDoS koruma yaklaşımdaki yeri büyüktür. Bir DDoS saldırısı gerçekleşmesi durumunda olay müdahalenin doğru ve etkin bir şekilde yapılabilmesi için olay yönetimi sürecinin sağlıklı bir şekilde hayata geçirilmiş olması gerekmektedir. Benzer şekilde olay müdahale yapacak, sistemlerde bir arıza oluşması durumunda geri dönüş çalışmalarını gerçekleştirecek ekibin de yetkin ve hazırlıklı olması önemli bir faktördür. Bu sebeple Acil Durum Eylem Planlarının hazırlanması, düzenli aralıklarla tatbikatlar aracılığıyla güncellik ve geçerlilik durumlarının kontrol edilmesi gereklidir.

DDoS Testleri

DDoS testleri, yukarıda bahsedilen DDoS koruma çalışmalarının belirli periyotlarda ve/veya önemli sistem/uygulama değişikleri sonrasında test edilmesi ve test sonuçlarına göre, yapılmış koruma çalışmalarının iyileştirmesine yönelik gerçekleştirilen faaliyetleri içerir.

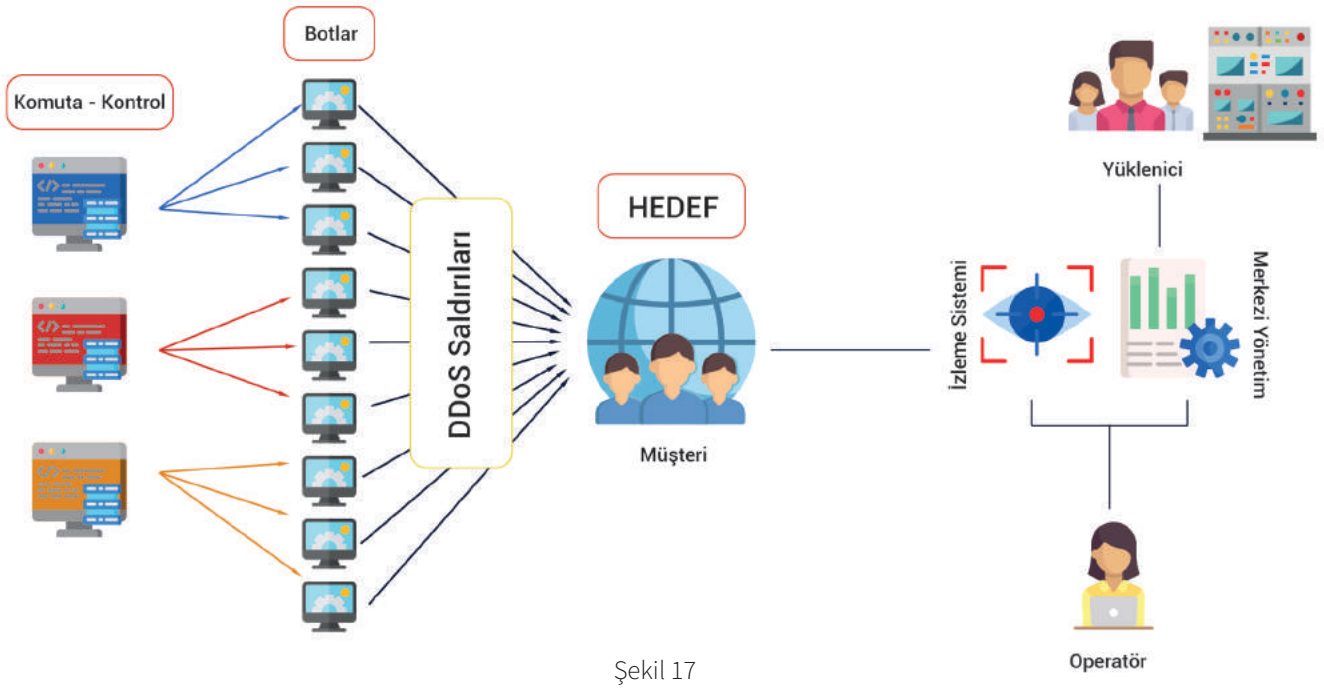
DDoS koruma yaklaşımı başlığında DDoS saldırılarından en az derecede etkilenmeye yönelik olarak gerçekleştirilmesi uygun olacak çalışmalardan bahsedilmiştir. Bahsi geçen insan-süreç-teknoloji

çalışmaları zaman ve para gerektirmekle birlikte, yatırım yapılmasını da gerektiren faaliyetleridir. Yapılan yatırımların gerçek bir saldırı olması durumunda ne derecede etkin ve verimli olduğunun ölçülmesi ve tespit edilen eksikliklerin giderilmesi önem arz etmektedir. Bu noktada gerçek saldırganların yaptığı gibi dünyanın farklı coğrafi bölgelerinden çok sayıda bot üzerinden yüksek miktarda trafik (bandwidth ve pps) üreterek, organizasyonun internete açık hizmetlerini test etmek gerekecektir. Özellikle internete açık uygulamaların sürekli olarak test edilmesi, mevcut uygulamalarda bir değişiklik yapılması veya yeni uygulamaların devreye alınması durumlarında bu testlerin tekrarlanması önemlidir.

LoDDoS

DDoS testlerinin yapılması için gerekli hazırlıkların yürütülmesi uzun süreli ve zahmetli bir iştir. Bu testlerin teknik ve yönetimsel hazırlık safhaları uzun sürmektedir. DDoS testinde kullanılacak sistemlerin hazırlanması ve yapılandırılması için hem güvenlik hem de BT ekiplerinin ortak çalışması gerekmektedir. Hazırlıklar tamamlandıktan sonra testin uygulanma aşamasında anlık izleme yapılamamakta, testler tamamlandıktan sonra raporların oluşturulması zaman almaktadır. İster bir kere isterse sürekli olarak yapılsın her test için hazırlık aşaması en baştan itibaren yapılmaktadır. Bu sebeplerle bu hazırlık ve ve uygulama aşamalarının bir uygulama aracılığıyla otomasyonunun sağlanması bir zaruriyet halini almıştır.

Bu noktada LoDDoS hizmet olarak sunulan bir DDoS Simülasyon ve Yük Testi platformudur. Bu platform organizasyonlara yapılacak olan DDoS saldırılarını gerçek saldırı parametreleri ile simüle eder. Ayrıca internete açık web uygulamalarının yüksek trafiklere karşı dayanıklılığını (resilience) ölçer.



Şekil 17

DDoS Simülasyonu sayesinde organizasyonlar gerçek bir DDoS saldırısına maruz kalmadan DDoS engelleme sistemlerinin sınırlarını ve yeteneklerini test edebilmektedir. Testler canlı olarak izlenebilir, kontrollü bir şekilde yapıldığından istenildiği zaman durdurulabilir, baştan başlatılabilir, anlık olarak raporlanabilir ve raporlar daha sonra değerlendirmek üzere saklanabilir.

Yük Testi özelliği sayesinde ise, web uygulamalarına yüksek sayıda istek gelmesi durumunda altyapılarının bu istekleri ne derecede karşılayabildiğini ölçümleyebilir ve gerçek bir yük durumu oluşmadan önce gerekli iyileştirmeleri yapabilirler.

Sonuçlar

DDoS saldırıları gün geçtikçe karmaşıklaşmakta ve daha büyük boyutlara ulaşmaktadır. DDoS saldırılarına uğramak organizasyonlar için kaçınılmaz bir hal almış olsa da, önlenemez saldırılar değildir. Saldırılar ne kadar büyük ve karmaşık olursa olsun, gerekli ve yeterli hazırlıklar yapıldığı durumda bu saldırılardan en az mertebede etkilenmek mümkün olabilmektedir. Yaşanmış Olaylar başlığı altında anlatılan örnek olaylar bu duruma en iyi örneklerdir. İnsan-Süreç-Teknoloji ekseninde gerçekleştirilen planlı savunma çalışmaları ile kurumların DDoS saldırılarına karşı dayanıklılığını arttırma noktasında önem arz eden faaliyetler olacaktır.

DDoS koruma ve savunma çalışmalarında yapılması gereken ana başlıkları özetleyecek olursak;

- *Dış, kenar ve orta katmanlarda gerekli olan güvenlik hizmet ve bileşenlerinin temin edilmesi, sürekli olarak izlenmesi ve iyileştirilmesi,*
- *DDoS korumaya yönelik süreç, prosedür ve talimatların oluşturulması ve güncel tutulması,*
- *DDoS korumada görevli personelin gerekli teknik ve idari eğitimleri alması,*
- *Önemli değişiklikler yapıldıktan sonra veya yeni uygulamalar devreye alınmadan önce veyahut periyodik olarak sistemlerin ve uygulamaların DDoS ve yük testlerine tabii tutulması,*
- *Tatbikatlar aracılığı ile insan-süreç-teknoloji bileşenlerinin belirli periyotlarla test edilmesi ve gerekli iyileştirmelerin uygulanması.*

LODDOS

Merkez Ofis

Mustafa Kemal Mahallesi,
Dumlupınar Bulvarı No:164,
Kentpark Ofis, Kat:4 Daire:06
Çankaya/Ankara

Telefon: +90 (312) 235 44 41
Fax: +90 (312) 235 44 51
E-posta: bilgi@barikat.com.tr

İstanbul Ofis

Nida Kule Ataşehir Kuzey İş Merkezi,
Barbaros Mahallesi, Begonya Sokak,
No:3, Daire: 71/72 Ataşehir/İstanbul

Telefon: +90 (216) 504 53 30
Fax: +90 (216) 504 53 32
E-posta: bilgi@barikat.com.tr

Amsterdam Ofis

Millenium Tower Floor 29,
Radarweg 29 1045 XN
Amsterdam/Netherlands

Telefon: +31 20 854 6146
E-posta: info@barikatbv.com