TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

DAĞITIK SERVİS DIŞI BIRAKMA SALDIRILARININ İNCELENMESİ VE KORUNMA YÖNTEMLERİ

Ersin MASUM

DİSİPLİNLERARASI ADLİ BİLİMLER ANABİLİM DALI
ADLİ BİLİŞİM
YÜKSEK LİSANS TEZİ

DANIŞMAN
Doç.Dr. Refik SAMET

ANKARA
2017

TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

DAĞITIK SERVİS DIŞI BIRAKMA SALDIRILARININ İNCELENMESİ VE KORUNMA YÖNTEMLERİ

Ersin MASUM

DİSİPLİNLERARASI ADLİ BİLİMLER ANABİLİM DALI
ADLİ BİLİŞİM
YÜKSEK LİSANS TEZİ

DANIŞMAN
Doç.Dr. Refik SAMET

ANKARA
2017

Ankara Üniversitesi
Sağlık Bilimleri Enstitüsü Müdürlüğü'ne,

Yüksek Lisans tezi olarak hazırlayıp sunduğum "DAĞITIK SERVİS DIŞI BIRAKMA SALDIRILARININ İNCELENMESİ VE KORUNMA YÖNTEMLERİ" başlıklı tez; bilimsel ahlak ve değerlere uygun olarak tarafımdan yazılmıştır. Tezimin fikir/hipotezi tümüyle tez danışmanım ve bana aittir. Tezde yer alan deneysel çalışma/araştırma tarafımdan yapılmış olup, tüm cümleler, yorumlar bana aittir.

Yukarıda belirtilen hususların doğruluğunu beyan ederim.

Öğrencinin Adı Soyadı : Ersin MASUM

Tarih : 22.07.2017

İmza :

Ankara Üniversitesi Sağlık Bilimleri Enstitüsü

Disiplinlerarası Adli Bilimler Anabilim Dalı,

Adli Bilişim Yüksek Lisans Programında

Ersin MASUM tarafından hazırlanan

"**DAĞITIK SERVİS DIŞI BIRAKMA SALDIRILARININ İNCELENMESİ VE KORUNMA YÖNTEMLERİ**" adlı tez çalışması

aşağıdaki jüri tarafından **YÜKSEK LİSANS TEZİ** olarak OY BİRLİĞİ ile kabul edilmiştir.

Tez Savunma Tarihi: 22 / 06 / 2017

Yrd.Doç.Dr. Hüseyin ÇAKIR
Gazi Üniversitesi Eğitim Fakültesi
Jüri Başkanı

Doç.Dr.Recep ERYİĞİT
Ankara Üniversitesi
Mühendislik Fakültesi
Üye

Doç.Dr.Refik SAMET
Ankara Üniversitesi
Mühendislik Fakültesi
Üye

Tez hakkında alınan jüri kararı, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü Yönetim Kurulu tarafından onaylanmıştır.

Prof. Dr. Mehmet AKAN
Sağlık Bilimleri Enstitüsü Müdürü Vekili

İÇİNDEKİLER

ÖNSÖZ

Siber teknolojinin hayatımızın her alanında kendilerine yer bulmayı başarması ile bilgisayar, mobil cihazlar, IoT, güvenlik kameraları ve akıllı cihazlar milyarlarca insanın kullandığı bir teknolojiye dönüşmüştür. Özellikle akıllı mobil cihazların internet, konum belirleme sistemleri (GPS), kablosuz iletişim ve sağlık uygulamaları gibi ileri düzey yetenek ve teknolojilerinin gelişimi ile yaşamımızın her anında yanımızdan ayıramadığımız bir parçamız olmaya başlamıştır. Kullanım oranının artması ile zararlı yazılım geliştiricilerin bu alana olan ilgisini arttırmıştır. Değişik konularda büyük bir kullanım yelpazesine sahip olan bu cihazlar, güvenlik açısından henüz gelişme döneminde olan mobil işletim sistemleri nedeniyle üzerine çalışmalar yapılması gözden kaçırılmaması gereken bir konudur. Bu çalışmada, dağıtık servis dışı bırakma saldırılarının incelenmesi ve korunma yöntemleri üzerinde geliştirilen sunucu yapısı ve mobil cihazların saldırı maksadıyla kullanımlarının tespitlerinin başarılı olup olmadığı konusunda incelemeler gerçekleştirdik.

Bilgisi ve sabrı ile örnek aldığım danışman hocam, Doç. Dr. Refik SAMET'e,

Bu çalışmanın hazırlanması aşamasında her türlü desteğini benden esirgemeyen, yaşama kaynağım olan oğlum Işık Kutay MASUM ve eşim Hülya MASUM'a,

Teşekkür eder, bu alana yönelmeme sebep olan Genelkurmay MEBS Başkanlığına bu tez çalışmasını atfederim.

SİMGELER VE KISALTMALAR

AMG	Alarm Matris Üreteci (Alarm Matrix Generator)
ANFIS	Uyarlanabilir Hibrit Nöro-Bulanık Çıkarım Sistemi (Adaptive And Hybrid Neuro-Fuzzy Inference Systems)
AS	Yönlendirme Alanına (Autonomous Segments)
BGP	Geçiş Protokolü (Border Gateway Protocol)
BOTNET	Köle Bilgisayar
C&C	Komuta ve Kontrol (Command & Control)
CAPTCHA	Ben Robot Değilim (Completely Automated Public Turing Test to Tell Computers And Humans Apart)
DoS	Servis Dışı Bırakma (Denial of Service)
DDoS	Dağıtık Servis Dışı Bırakma (Distributed Denial of Service)
FTP	Dosya Aktarım Protokolü (File Transfer Protocol)
GPS	Coğrafi Konum Sistem (Global Positioning System)
HIDS	Bilgisayar Tabanlı Saldırı Algılama Sistemi (Host-based Intrusion Detection System)
ICMP	Internet Kontrol Mesajı Protokolü (Internet Control Message Protocol)
IDS	Saldırı Algılama Sistemi (Intrusion Detection System),
IMEI	Uluslararası Mobil Cihaz Kimliği (International Mobile Equipment Identity)
IoT	Nesnelerin İnterneti (Internet of Things)
IP	Internet Protokolü (Internet Protocol)
IPS	Saldırı Önleme Sistemi (Intrusion Prevention System)
IRC	İnternet Aktarmalı Sohbet (Internet Relay Chat)
IRS	Yetkisiz Giriş Tespit Sistemi (Intrusion Response System)
ISO	Uluslararası Standartlar Teşkilâtı (International Organization for Standardization)
MCA	Çok Değişkenli Korelasyon Analizi (Multivariate Correlation Analysis)
ML	Makine Öğrenme (Machine Learning)
OSI	Açık Sistem Bağlantıları (Open Systems Interconnection)
RAS	Risk Değerlendirme Sistemi (Risk Assessment System)
SAR	SYN Varış Oranı (SYN Arrival Rate)
SAVE	Kaynak Adresi Doğrulama Uygulama (Source Address Validity Enforcement)
SPAM	İstenmeyen E-posta
TCP	İletim Kontrol Protokolü (Transmission Control Protocol)
UDP	Kullanıcı Veri bloğu Protokolü (User Datagram Protocol)

ŞEKİLLER

1. GİRİŞ

Bilgisayar ağları üzerinde dijitalleştirilmiş bilginin iletildiği düşünsel ortam olarak tanımlanan siber uzay bir zamanlar sadece iletişim ve sonrasında e-ticaret dünyasında iken, günümüz medeniyetinin yürümesini sağlayan tarım-gıda dağıtımından bankacılık, sağlık, ulaşım, su ve enerjiye kadar değişen birçok sektör de kullanılmaktadır. Bu sektörler bir zamanlar bağımsız değerlendirilirken şimdi hepsi birbirine bağlı ve siber uzaya bilgi teknolojileri vasıtasıyla, çoğunlukla "uzaktan kontrol ve gözetleme sistemi" SCADA üzerinden bağlıdırlar. Siber uzay; şehir suyunun klor seviyesini dengeleyen, evinizi ısıtan gazın akışını kontrol eden, borsa ve finansal işlemleri yapmak için kullanılan 21'nci yüzyılın yaşam platformudur (Spreitzenbarth, 2017). Siber uzay, bireylerin ve toplumların günlük yaşamlarında çok önemli faydalar ve kolaylıklar sağlamaya başlamış olsa da zararlı ve bilinçsiz kullanımdan dolayı bazı dezavantajları da beraberinde bulundurmaktadır (Gürkaynak, 2011). Teknolojinin hızla ilerlemesine karşın, bu teknolojileri istismar etme yöntemleri ve teknikleri her geçen gün gelişmektedir. Bu durum bazen bir ülkeyi elektriksiz, bir şehri susuz veya trafik karışıklığı ile karşı karşıya bırakabilmektedir.

Siber terörizm, siber alan ve siber savaş gibi kavramların uluslararası sistemde kabul görmüş tanımları yoktur. Bununla birlikte siber savaş için de bazı tanımlar yapılmıştır. ABD Savunma Bakanlığı siber savaşı, "saldırıyı düzenleyenlerin temel amaçlarına ulaşmak için sahip oldukları siber kapasitenin siber alanda kullanılması" olarak tanımlamıştır (USA Department Of Defence, 2017). Siber alanda gerçekleştirilen saldırıların geleneksel saldırılardan önemli farklılıkları bulunmaktadır. Her şeyden önce siber savaş ışık hızı gibi yüksek bir hızda gerçekleştirilebilme olanağına sahip ve asimetriktir. Bununla birlikte modern toplumlardaki altyapının yüksek teknolojiye ihtiyaç duyması nedeniyle, sanal dünya üzerinden gerçekleştirilen saldırıların etkileri konvansiyonel silahlar kadar büyük

olabilmektedir. Ayrıca siber saldırıların maliyeti geleneksel saldırılarla mukayese edilemeyecek kadar düşük ve siber saldırının hedefinde yer alan objenin kasten mi yoksa kazayla mı saldırıya maruz kaldığının anlaşılması kolay değildir (Todd, 2009).

Siber alanda gerçekleşen saldırıların ve savaşların kendine özgü silahları bulunmaktadır. Bu silahlar doğrudan fiziki dünyayı hedef almasalar da sanal dünya ile bütünleşmiş günlük hayatta da olumsuz sonuçlara yol açabilmektedirler. Örneğin, ulusal haberleşme ağlarına zarar verebilmekte veya elektrik santrallerini devre dışı bırakarak kullanılamaz hale getirebilmektedirler. 2015 yılında Türkiye'de neredeyse bütün ülkeyi kapsayan büyüklükte elektrik kesintisi olmuş ve bu kesintinin nedeni olarak siber saldırılar gösterilmektedir (Ntv, 2017).

Siber silahları iki başlıkta toplamak mümkündür. Bu silahlar genel olarak sözdizimsel (Syntactic) ve anlamsal (Semantic) tipteki silahlar olarak adlandırılmaktadır (Brenner ve Goodman, 2002). Sözdizimsel silah DDoS (Distributed Denial of Service) saldırılarını ve zararlı yazılımlar (Malicious Code, Spyware, Trojan Horses ve Worms) kullanarak bilgisayarların işletim sistemlerine zarar verirler. Anlamsal siber silahlar ise bilgisayarda karşımıza çıkan bilgilerin doğruluğunu değiştirerek bilgisayar kullanıcılarına kendini fark ettirmeden yanlış bilgi edinmelerini sağlarlar.

Sözdizimsel siber silahın en önemli unsuru olan DoS/DDoS saldırılarındaki amaç kritik bilgileri çalmak, onları düzenlemek veya yok etmek değildir; DoS saldırıları herhangi bir ağın işleyişini bozmaya yönelik saldırılardır (Xiang ve ark., 2010). DDoS saldırıları ise virüsler tarafından etki altına alınmış çok sayıda bilgisayar veya akıllı cihazın tek bir bilgisayar, sunucu ve web sayfasına saldırmasıdır. Saldırgan bu sayede, binlerce bilgisayarın aynı anda tek bir sunucuya saldırmasını organize ederek onu etkisiz hale getirebilmektedir (Douligeris ve Mitrokotsa, 2003). ANDROID ve iOS işletim sisteminin geliştirilmesi ile

kullanılmaya başlanan akıllı mobil cihazlar ve akıllı olmayan cihazların bu saldırılarda kullanılması saldırının boyutunun karşı konulmaz büyüklüğe ulaşmasını sağlamaktadır. Son zamanlarda Dyn DNS sağlayıcısına yapılan saldırılarda görüldüğü gibi, nesnelerin interneti (IoT) BOTNET saldırıları kullanılarak güçlendirilmiş DDoS saldırıları 2016 yılında olduğu gibi 2017'de de gerçekleşmeye devam edecektir. Mirai tarafından 19 Eylül 2016 tarihinde Fransız merkezli bir hosting firması olan OVH'yi hedef alan ve IoT BOTNET ile gerçekleştirilen DDoS saldırısı, bir saniyede 1 Terabit gibi devasa bir trafiğe ulaşmıştır (STM, 2016). Bu saldırının en büyük özelliği; 150.000'i aşkın sayıda, büyük bir bölümü IP kamera, ufak işlemci gücüne sahip internete bağlanabilen elektronik cihaz ve akıllı telefonlar kullanılarak gerçekleştirilmesidir. Şu anda mevcut bilgi sistem teknolojileri ile bir saniyede 1 Terabit boyutundaki DDoS saldırısına karşı koyabilecek herhangi bir güvenlik sistemi bulunmamaktadır. Bu durum bir kişi veya grubun en güçlü devlet aktörleri için hazırlanmış dünya çapında bir siber silaha sahip olmasını sağlamaktadır. IoT'lar BOTNET teknolojisinin büyümesinde en büyük etken ve güvenlik konusu pek fazla düşünülmeden üretilen cihazlardır. Güvenlik güncellemesi mevcut olan milyonlarca hassas IoT cihazı bulunmakta, ancak güncelleme işlemi o kadar karışıktır ki, kullanıcılar güncelleme işlemini ertelemeyi tercih etmektedir (IoT, 2017)

Bilgi güvenliği ise, bilgilerin izinsiz erişimlerden, kullanımından, ifşa edilmesinden, yok edilmesinden, değiştirilmesinden veya hasar verilmesinden korunması işlemidir. Mahremiyetin, bütünlüğün ve bilginin ulaşılabilirliğinin korunması hususu ortak hedeftir. Temel güvenlik fonksiyonları aşağıdaki şekilde sıralanabilir (BİLGEM, 2015).

- Kimlik Sınaması (Authentication)
- Yetkilendirme (Authorization)
- İzlenebilirlik/Kayıt Tutma (Accountability)
- Gizlilik (Confidentiality)

- Veri Bütünlüğü (Data Integrity)
- Güvenilirlik (Reliability-Consistency)
- İnkâr Edememe (Non-repudiation)
- Süreklilik (Availability)

DDoS saldırıları yukarıda bahsedilen bilgi güvenliği unsurlarından sürekliliği hedef almaktadır. Süreklilik; bilginin her an ulaşılabilir ve kullanılabilir olmasını amaçlayan prensiptir. Bilişim ile desteklenen sektörlerin sürekli bir şekilde tam ve eksiksiz olarak hizmetin devam etmesi amaçlanmaktadır. Bilişim sistemlerinin kurum içinden ve dışından gelebilecek tehditlere karşı korumayı süreklilik sayesinde sağlanmaktadır. Süreklilik hizmeti sayesinde, verilerin güncelliğini yitirmeden, zamanında ve güvenilir bir şekilde ulaşılması sağlanmaktadır.

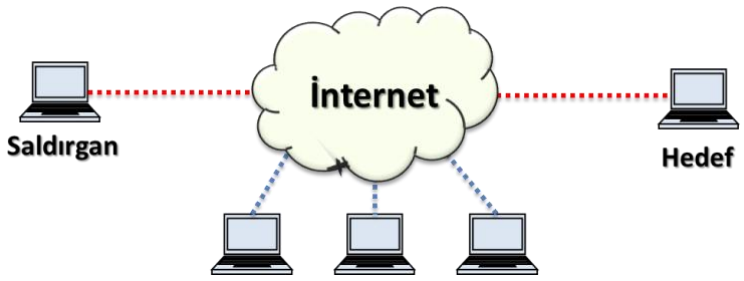
Bu tez çalışmasında; son yıllarda gerçekleşen çeşitli DOS/DDoS saldırıları analiz edilerek, tespit yöntemleri incenmiş, kullanılan araçlar araştırılmış ve saldırı öncesinde alınabilecek tedbirler ortaya konulmuştur. Yapılan incelemede; son yıllarda yapılan DDoS saldırıların neredeyse tamamında mobil cihazlar kullanılarak yapıldığı tespit edilmiş olması nedeniyle bu çalışmada mobil cihazlar üzerinde yoğunlaşılmıştır. Bu kapsamda; DoS/DDoS temel tanım ve kavramları açıklandıktan sonra mobil BOTNET saldırıları, hâlihazırda mevcut BOTNET ailelerinin analizi ve DDoS maksadıyla kullanımı örnekler ile sunulmuştur. Ayrıca BOTNET saldırılarının DDoS amaçlı olarak kullanımı araştırılmış, BOTNET saldırılarının ortak özellikleri belirlenmiş, bu özelliklerle BOTNET modelleme adımları arasındaki ilişki saptanmış, uygulamalarda söz konusu özelliklerin tespit yöntemleri ve DoS/DDoS ile BOTNET saldırılarından korunmak maksadıyla sunucu mimarisi önerilmiştir.

1.1. Servis Dışı Bırakma ve BOTNET Saldırıları

Bu bölümde, DDoS saldırılarının genel tanımı, amacı, hedefleri, hâlihazırda mevcut BOTNET ailelerinin DDoS maksadıyla kullanımı, türleri ve kullanılan araçlar hakkında temel kavram ve tanımlar sunulmuştur.

1.1.1. DOS: Servis Dışı Bırakma (Denial of Service)

DoS; sistemin ya da servislerin aşırı yüklenmesini sağlayarak hizmet veremez hale gelmelerini hedefleyen bir saldırı türüdür. Bu saldırı türünde hedef internet uygulamasının kendisi değil uygulamayı barındıran sunucu ve kaynaklardır. DoS saldırıları sonucunda sunucular ya da sistemler hizmet dışı bırakılabilir. Bunun sonucunda uygulama sahibi şirket ya da kişi; iş kaybı, maddi kayıp ve itibar kaybı yaşayabilir. Şekil 1.1'de görüldüğü üzere DoS saldırıları tek bir merkezden yine tek bir merkeze yapılan saldırılar olarak adlandırılır (Çelikbilek, 2016).



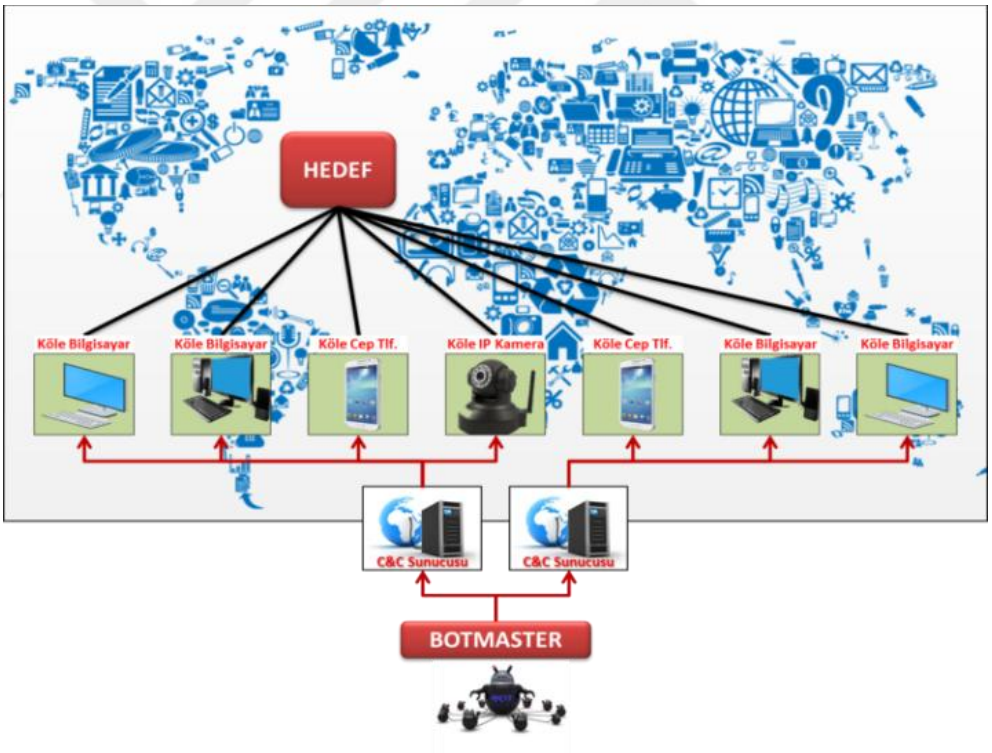
Şekil 1.1. DOS saldırı senaryosu

1.1.2. DDoS: Dağıtık Servis Dışı Bırakma (Distributed Denial of Service)

DDoS; İnternet üzerinden ele geçirilen birden fazla sistemden tek bir noktaya yapılan servis dışı bırakma saldırıları olarak tanımlanabilir. Bu tür saldırıların asıl

amacı bilgi güvenliğinin en önemli yapı taşı olan erişilebilirlik ve sürekliliği ortadan kaldırılmasıdır. DDoS saldırılarını DoS saldırılarından ayıran en önemli fark ise birden fazla noktadan tek bir noktaya aynı anda yapılmasıdır. Tek bir noktaya yapılan bu saldırılarda on binlerce köle bilgisayar taşeron olarak kullanılabilmektedir.

DDoS saldırı çeşidinde farklı noktalardan sunucuya eş zamanlı olarak çok sayıda veri paketi gönderilir. Sunucu kendisine gönderilen paketleri işlerken kendi sistem kaynaklarını (işlemci, hafıza, bant genişliği) tüketebilir. DDoS saldırılarının temel amacı hedef sistemin bant genişliğini ya da kaynaklarını (CPU, RAM, Disk) tüketmektir. Sonuç olarak sunucu veri paketlerine cevap veremez hale geldiğinde servis dışı kalmış olacaktır. Şekil 1.2'de DDoS saldırı senaryosu görülmektedir.



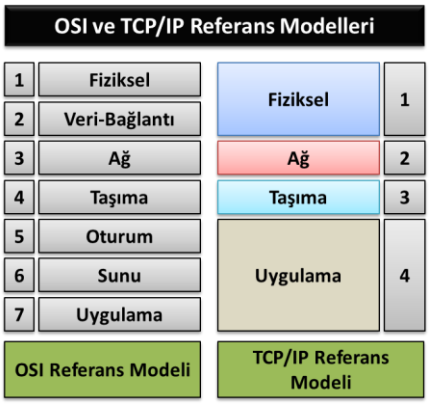
Şekil 1.2. DDoS saldırı senaryosu

DDoS saldırılarının anlaşılması için öncelikle OSI ve TCP/IP Referans Modellerinin incelenmesinde fayda vardır.

1.1.3. OSI ve TCP/IP Referans Modelleri

İnternetteki ya da genel olarak ağlardaki aktif cihazların birbirleri ile görüşebilmeleri için OSI (Open Systems Interconnection) referans modeli geliştirilmiştir. Bu model sayesinde ağdaki aktif cihazlar üzerinde bulunan uygulamaların birbirleri ile nasıl iletişim kuracağı tanımlanmıştır (Briscoe, 2000). 1978 yılında ilk defa ortaya çıkarılan bu standart 1984 yılında yeni bir düzenleme yardımıyla OSI referans modeli olarak yayınlanmıştır. Bilgisayar dünyasının ilk yıllarında ayrı ayrı yapılardan oluşması ve her firmanın kendi marka cihazlarının haberleşmesi için kendi modelini ortaya koyması bu standartlaşmaya gidilmesine neden olmuştur. ISO (International Organization for Standardization) farklı marka cihazların birbiri ile iletişimini sağlamak amacıyla OSI referans modelini ortaya çıkarmış ve herkesin bu model doğrultusunda cihazlar üretmesine neden olmuştur. Diğer bir model ise TCP/IP referans modelidir.

OSI referans modelindeki 7 katmana karşılık TCP/IP referans modeli 4 katmanlı bir çözüm sunar ve 7 katmanlı OSI modeline göre daha hızlı bir iletişim imkânı sunmaktadır. OSI modeli iletişim standartlarını belirlemeye yönelik, TCP/IP uygulanabilir bir model olduğu için daha çok uygulamaya yöneliktir. Veriler bu katmanları izleyerek bir yerden diğerine iletilmektedir. Her bir katmanın kendi içerisinde diğer katmanlardan ayrı olarak kendine özgü görevleri tanımlanmıştır. Ağ mimarisinin her katmanında bir problem ile karşılaşıldığında log (iz kaydı) kayıtları incelenerek problemlere çözüm bulunmaktadır. DDoS saldırılarında TCP/IP referans modelindeki her katmana özgü saldırı çeşidinin olması her bir katmanın ayrıca incelenmesine ihtiyaç vardır. OSI ve TCP/IP referans modelleri Şekil 1.3'de gösterilmiştir. Bu bölümde TCP/IP referans modeli katmanları anlaşılması daha kolay olması için geriden başa doğru anlatılmaktadır.



Şekil 1.3. OSI ve TCP/IP referans modeli

TCP/IP birçok protokolün toplandığı bir protokoller ailesidir. Bu referans modeline en çok kullanılan iki protokolün ismi verilmiştir; TCP (Transmission Control Protocol) ve IP (Internet Protocol). Bu referans modelinde 4 farklı katmanda 15'ten fazla protokol vardır. Veriler bu katmanlar arasında sırasıyla paketlenerek gönderilir, alıcıda ise paketlemenin tersi sırayla teker teker açılarak veri iletilmektedir.

1.1.3.1. Uygulama Katmanı

Bu katmanda gönderilecek veri tipi ve veriyi işleyen uygulamalar bulunur. Örneğin bir HTML web sayfası ve bu veri tipini kullanan HTTP protokolü bu katmandadır. OSI modelindeki sunum ve oturum katmanları TCP/IP modelinde uygulama katmanı içerisinde yer alır. E-Posta gönderimi için kullanılan SMTP ve dosya gönderimi için kullanılan FTP protokolleri bu katmanda bulunur (Kaplan, 2000). Uygulama katmanı saldırısında, saldırgan trafiği hedefe yönlendirmek için HTTP ve HTTPS gibi uygulama katmanı protokollerini kullanılır. Bu tür trafikte normal olarak hedef sunucu CPU'na yoğun sorgular gönderilir ve onu cevap veremez hale gelene kadar meşgul etmesi sağlanır. Bir uygulama katmanı saldırı trafiğinin, meşru trafiğinden ayırt edilemez olması saldırının ayırt edilmesini zorlaştırır.

1.1.3.2. Taşıma Katmanı

Bu katmanda verinin nasıl gönderileceği belirlenir. Veri güvenliği ve hata kontrolü gibi işlemler yapılır. TCP ve UDP protokolleri bu katmandadır. TCP klasik veri aktarımında UDP ise medya aktarımında kullanılır. TCP, UDP'ye göre daha güvenli fakat daha yavaş çalışır. Çünkü TCP'de gönderilen her veri paketinin ardından verinin yerine doğru bir şekilde ulaşıp ulaşmadığı kontrol edilir (Kaplan, 2000). Ağ veya taşıma katmanı saldırısı sırasında, saldırgan, ağ trafiğini sağlayan Router ve Switch gibi aygıtların bellek ve CPU gibi kaynaklarını tüketmeye çalışır. Bu amaca ulaşmak için üç ve dördüncü katmandaki cihazlara büyük yoğunlukta trafik isteği gönderirler. Böyle bir saldırı, genellikle birkaç Gbps'den 1 Tbps'ye kadar olan hacimlere ulaşmaktadır.

1.1.3.3. Ağ Katmanı

IP katmanı olarak da adlandırılan bu katman da verilerin gideceği adres veriye eklenir yani veri bu katmandan gönderilir ve yönlendirilir. IPv4 ün gelecekte yetersiz kalma durumuna karşı IPv6 sistemine geçmek için çalışmalar başlatılmıştır.IPv4 32 bit iken IPv6 ile 128 bitlik adresler kullanılacaktır. Bu sayede daha fazla IP adresi atanabilecektir (Kaplan, 2000).

1.1.3.4. Fiziksel Katman

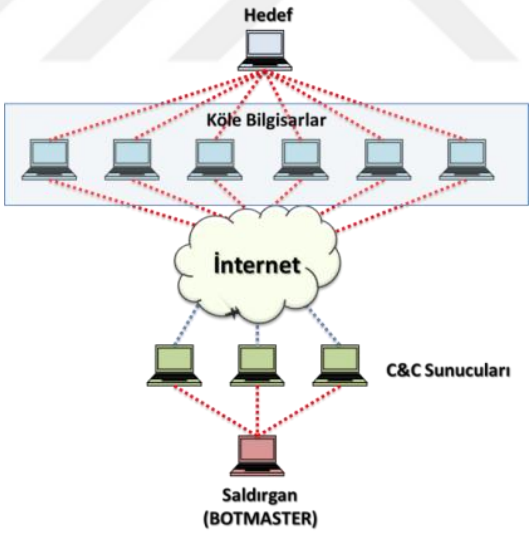
Bu katmanda verinin hangi yolla gönderileceği belirlenir. İletişim ortamının özellikleri, haberleşme hızı ve kodlama şeması belirlenir. Ethernet, Wi-Fi ve ATM gibi protokoller bu katmanda çalışır. Bu katmanda haberleşmek için kablosuz ortam da kullanırlar. Bu ortam birçok DoS tipi saldırıya maruz kalabilmektedir. Frekans

Bozumu (Jamming) Saldırısı ve cihazlara fiziksel olarak erişim ile ayarların bozulması örnek olarak verilebilir.

1.1.4. DDoS Saldırı Aşamaları

Genellikle, DDoS saldırısı DoS saldırısından daha zararlı olarak kabul edilir. DDoS saldırısı oluşturmak için daha fazla planlama ve özen gerekmektedir. DDoS saldırısı dört adımdan oluşur;

1. Saldırgan ağ üzerinden savunmasız kullanıcıları tarar,
2. Güvenlik açığı bulunan sunucular zararlı yazılım marifetiyle ele geçirilir,
3. Saldırgan saldırıyı etkili bir şekilde başlatmak için ele geçirilmiş makinaları kullanır,
4. Komuta Kontrol sunucuları ile saldırı başlatılır (Şekil 1.4).



Şekil 1.4. DDoS saldırı aşamaları

BOTMASTER tarafından saldırının başlatılması için, komuta kontrol sunucuları ile iletişime geçerek diğer köle bilgisayarlara komut gönderir. İlk önce zararlı yazılım internete yüklenir ve bu yüklemeler ana unsur olarak kullanılır. Bu

yazılımlar, köle bilgisayarlarla mesaj alışverişi yapmak için kullanılır. İlginçtir ki, bu zararlı yazılımın varlığı ve köle bilgisayar ile hedef arasındaki iletişim, sistem sahipleri ve kullanıcıları tarafından bilinmemektedir. İletişim için İnternet Aktarmalı Sohbet (IRC: Internet Relay Chat) kanalı kullanılır.

1.1.5. DDoS Saldırı Türleri

DDoS saldırı çeşitli araştırmacılar tarafından farklı ölçütleri izleyen farklı yollarla sınıflandırılmış çeşitli görüşler mevcuttur. Bazı kaynaklar DDoS saldırılarını OSI katmanları ile sınıflandırırken bazı kaynaklar kullanılan araç ve yöntemlere göre bazıları ise de etkilerine göre sınıflandırmaktadır (Hoque, 2013). Bu bölümde yoğunluk (Volume-based) ve protokol (Layer-Based) tabanlı DDoS saldırıları incelenmiştir.

1.1.5.1. Yoğunluk Tabanlı Saldırılar

Yoğunluk tabanlı saldırılarında amaç hedefin herhangi bir servisine yönelik bant genişliğinin tüketilmesidir. Bu saldırı türünde hedefe doğru yapılan istekler de BOTNET'e dâhil olmuş ve bulut sistemi içerisindeki sunucular kullanılarak çok sayıdaki sistemden yapılan saldırılardır.

Saldırısı anında alınacak log'larda en belirgin husus kaynak IP adreslerinin çoğunlukta olmasıdır. Kullanılan IP'ler çoğunlukla sahtedir. Bu IP adreslerine Spoof edilmiş IP adresleri olarak adlandırılır. Bu IP adresleri zararlı yazılım bulaşması sonucu BOTNET'e dâhil olmuş ve BOTMASTER tarafından (IRC) kontrol edilen köle bilgisayarlardır. DDoS saldırılarında çoğunlukla saldırı kaynağının gizlenmesi için C&C sunucuları kullanılır. BOTNET'e dâhil olan köle bilgisayar sahipleri çoğu zaman bu sürecin farkında bile değillerdir. Kullanıcılar sadece; bilgisayar üzerine

gözlemlenen yavaşlamalar, internette sürekli paket gönderildiğinde ve internet adil kullanım kotasının çok çabuk dolması durumunda bu durumdan şüphelenmektedirler.

Mirkovic ve ark. (2004) yoğunluk tabanlı DDoS saldırılarını dört kategoriye ayırmıştır;

a) Sabit hız saldırısı: Saldırı oranı, çok kısa sürede maksimuma ulaşır. Tüm köle bilgisayarlar saldırı komutu aldıktan sonra, saldırı trafiğini sabit bir oranda göndermeye başlar.

b) Artan hız saldırısı: Hedefe tam ve sabit güçle saldırmak yerine, saldırgan trafik yoğunluğunu saldırgana doğru kademeli olarak artırır. Saldırgan, hedefin bant genişliği kapasitesini anlamak için artan oranda bir saldırı yaklaşımını benimsemekte; böylece saldırgan hedefin savunma mekanizmalarından kaçmayı amaçlamaktadır.

c) Darbeli saldırı: Saldırgan, bu tür bir saldırıda, periyodik olarak hedefe saldırı trafiğini göndermek için bir grup BOT aktifleştirir. Bu yöntem DDoS savunma mekanizması tarafından algılanmaması için kullanılır. TCP yeniden iletim zamanaşımı mekanizmasındaki açıklıktan istifade ederek yapılan bir DDoS saldırı örneğidir.

d) Alt grup saldırısı: Darbeli bir saldırı durumunda olduğu gibi burada da saldırgan, hedefe bir saldırı darbesi gönderir. Bununla birlikte, köle bilgisayarlar gruplara ayrılır ve bu gruplar farklı kombinasyonlarda aktive edilir ve tekrardan deaktive edilir. Böyle bir alt grup gizliliği ve saldırıyı daha uzun süre devam ettirmeye yönelik olarak kullanılır (Mirkovic ve ark., 2004).

1.1.5.2. Protokol Tabanlı Saldırılar

OSI katmanları açısından servis dışı bırakma saldırıları; uygulama katmanı ve ağ katmanı DDoS saldırıları olarak iki kategoriye sınıflandırılabilir. OSI katmanlarından yedincisi olan uygulama katmanı saldırısında, saldırgan trafiği

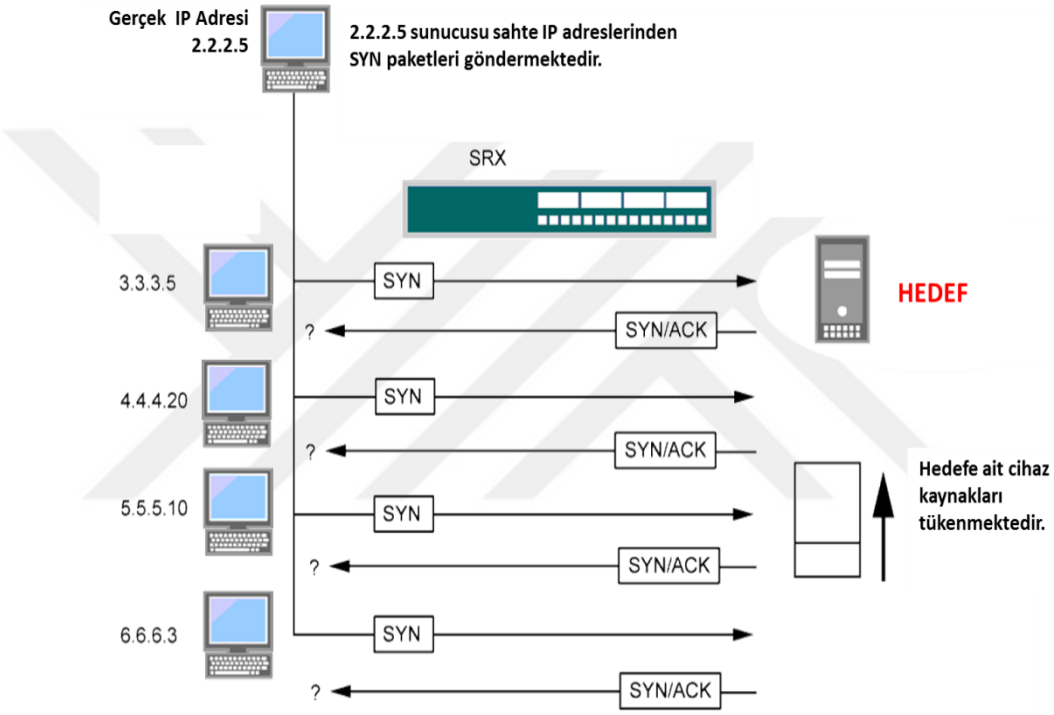
hedefe yönlendirmek için HTTP ve HTTPS gibi uygulama katmanı protokollerini kullanılır. Bu tür trafikte normal olarak hedef sunucu CPU'na yoğun sorgular gönderilir ve onu sonsuza kadar meşgul etmesi sağlanır. Bir uygulama katmanı saldırı trafiğinin, meşru trafiğinden ayırt edilemez olması saldırının ayırt edilmesini zorlaştırır.

Ağ veya taşıma katmanı saldırısı sırasında, saldırgan, ağ trafiğini sağlayan Router ve switch gibi aygıtların bellek ve CPU gibi kaynaklarını tüketmeye çalışır. Bu amaca ulaşmak için; 3. ve 4. katmandaki cihazlara büyük yoğunlukta trafik isteği gönderirler. Böyle bir saldırı, genellikle birkaç Gbps 'den 1 Tbps'ye kadar olan hacimlere ulaşmaktadır. Böyle bir saldırıda Internet Kontrol Mesajı Protokolü (ICMP), Kullanıcı Veri bloğu Protokolü (UDP: User Datagram Protocol) ve İletim Kontrol Protokolü (TCP: Transmission Control Protocol) gibi farklı ağ katmanı protokolleri kullanılır. En çok kullanılan ağ katmanı DDoS saldırıları, TCP SYN Flooding, HTTP GET Flooding, ICMP Flooding, UDP Flooding ve DNS Yükseltme (Amplification)'dir.

1.1.5.2.1 TCP SYN Flooding Saldırısı

OSI ve TCP/IP referans modellerinde açıklandığı gibi bilgisayarlar kendi aralarında bağlantı kurabilmesi için iletişime geçerler. Bu iletişim protokolleri tasarım hataları nedenleri ile saldırganlar tarafından istismar edilirler. Saldırgan ilk önce, rastgele kaynak adrese sahip SYN bayraklı paketleri hedef sisteme gönderir. Hedef sisteme ulaşan SYN paketlerine sunucu SYN-ACK paketi ile karşılık verir. Fakat kaynak adresi rastgele olarak ayarlandığı için sunucunun gönderdiği paketler atağın gerçekleştirildiği sisteme gitmeyecektir. Sunucunun gönderdiği SYN-ACK paketi eğer kaynağı rastgele oluşturulmuş sisteme ulaşırsa, paketi alan sistem böyle bir oturum bilgisinin kendisinde olmadığını hedef sisteme RST paketi göndererek belirtir. Hedef sistem bu paketi alınca oturumu hemen kapatır. Fakat SYN-ACK

paketi kaynak adresi rastgele oluşturulmuş sisteme ulaşamazsa hedef sistem bir süre bekledikten sonra paketin yolda kaybolmuş olacağını düşünerek tekrar SYN-ACK paketi gönderir. Bu bir süre böyle devam ettirildiğinde sunucu üzerinde yarım açık bağlantılar kurulmuş olur. Eğer saldırgan sunucu üzerinde yeteri kadar yarım açık bağlantı kurabilirse kaynakları tükeneceği için sunucu kendisine gelen legal isteklere cevap veremeyecektir (BİLGEM, 2015). Tasarıma dayalı istismar örneklerinden biri olan TCP SYN Flooding saldırısına ait mimari Şekil 1.5'de gösterilmektedir.



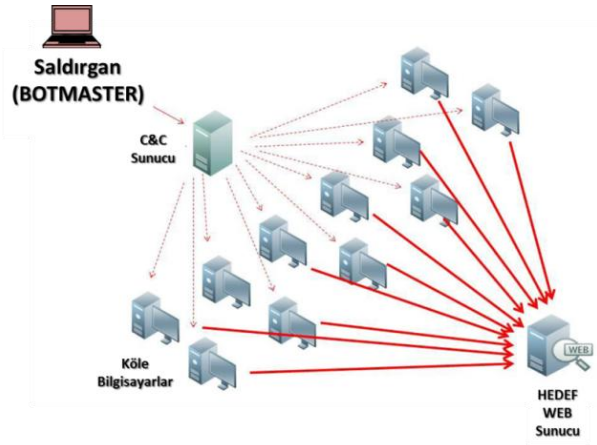
Şekil 1.5 TCP SYN Flooding saldırısı (BİLGEM, 2015).

Çözüm olarak internet çıkışında yer alan yönlendiricide uRPF (Unicast Reverse Path Forwarding) özelliği etkinleştirilmişse üretilen sahte paketlerin yönlendiriciden çıkışı engelleneceği için hedef sisteme herhangi bir etki ulaşmayacaktır. uRPF'teki temel mantık paketin kaynak IP adresinin yönlendirme tablosu ile karşılaştırılarak uygun arabirimden gelip gelmediğinin kontrolü sonucu paketin düşürülmesidir.

Sistem üzerinden yapılacak ayarlar ile bu tür saldırıların etkisi azaltılabilir. Örneğin açılabilecek en fazla yarı açık (half-open) bağlantı sayısı arttırılabilir. Linux işletim sistemlerinde en fazla olabilecek yarı açık bağlantı (sysctl net.ipv4.ip_local_port_range = 15000 61000) komutu ile ayarlanabilir. Ayrıca yarı açık bağlantılarda bekleme süresi kısaltılabilir. Linux işletim sistemlerinde şu şekilde bir komut ile yarı açık bağlantılarda bekleme süresi 60 saniye ile sınırlandırılmış olur (net.ipv4.tcp_fin_timeout = 60). En çok tercih edilen koruma tedbirlerinden biriside; SYN Cookie ve SYN Proxy'dir.

1.1.5.2.2 HTTP GET Flooding Saldırısı

TCP oturumunun kurulması için gerekli üçlü el sıkışmanın tamamlanması için bağlantının gerçek IP adreslerinden kurulması gerekir. Web sunucuyu servis dışı bırakarak web sayfasının işlevsiz kalması ve o sayfa üzerinden verilen hizmetlerin kesintiye uğraması amacıyla gerçekleştirilebilecek bir HTTP GET akış saldırısında sahte olmayan IP adresleri ile bir ya da birden fazla makineden eşzamanlı olarak çok sayıda istek gönderilir (BİLGEM, 2015). HTTP GET Flooding saldırı mimarisi Şekil 1.6'da sunulmuştur.

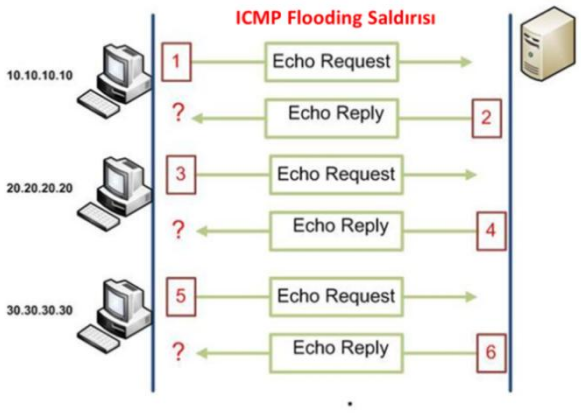


Şekil 1.6. HTTP GET flooding saldırısı (BİLGEM, 2015).

Bir IP adresinin açabileceği oturum sayısının kısıtlanması HTTP GET Flooding saldırılarına karşı alınabilecek önlemlerin en önemlisidir. Belirli bir oturum sayısını geçen IP adreslerinin kara listeye alınması HTTP GET Flooding saldırısına karşı alınabilecek diğer bir önlemdir. BOTNET'e dâhil olduğu bilinen IP adresleri saldırı anında kara listeye alınıp, bağlantıları düşürülebilir. Ayrıca pfSense üzerinde, saldırı sırasında BOTNET'e dâhil olduğu bilinen IP adresler kara listeye alınıp düşürülebilir.

1.1.5.2.3 ICMP Flooding Saldırısı

Bu saldırı türünde; Şekil 1.7'de görüldüğü gibi saldırgan tarafından hedef sisteme gönderilen ICMP Echo Request paketlerine karşılık hedef sistem ICMP Echo Reply paketi ile cevap verir. Bu sistem tasarımından faydalanan saldırgan, çok sayıda ICMP Echo Request paketi gönderir. Hedef sistem, gelen tüm bu isteklere cevap vermek için çaba harcar ve sistem kaynakları bunlara cevap veremez hale gelerek erişilemez olur.



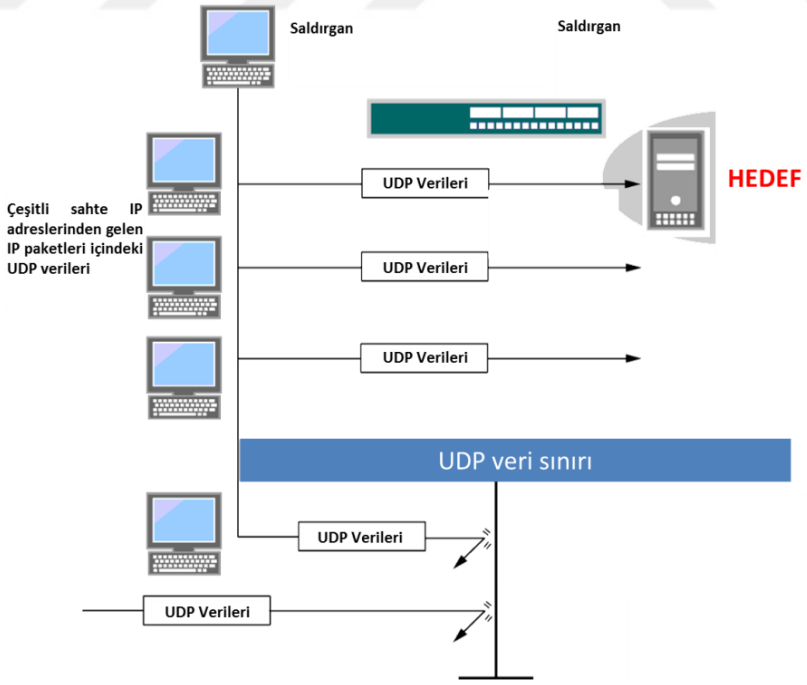
Şekil 1.7. ICMP flooding saldırısı (Antoniou, 2009).

Önlem olarak ICMP paketlerine cevap vermesi gerekli olmayan sunucuların bu paketlere cevap verme özelliği kapatılmalıdır.

1.1.5.2.4 UDP Flooding Saldırısı

Bu saldırı iki şekilde gerçekleştirilebilir. Birincisi hedef üzerinde açık UDP portu varsa bu port'da çalışan uygulama şekil bozukluğuna uğratılmış ve rastgele kaynak adresli oluşturulmuş UDP paketleri hedefe gönderilerek sunucu üzerinde çalışan servisin işleyişinin sekteye uğratılması sağlanır.

Diğer yöntemde ise, hedef sistem üzerinde açık UDP portu üzerinde çalışan bir uygulamanın olmadığı durumda sunucunun açık olan UDP portuna rastgele kaynaklı UDP paketleri gönderilir. UDP paketlerini alan hedef bu port üzerinde bir uygulamanın çalışmadığını belirtmek için UDP protokolünün bir özelliği olarak "ICMP port unreachable" paketi ile cevap verir. Bu şekilde sunucu üzerinde bir yoğunluk oluşturup cevap veremez hale gelmesi hedeflenmektedir. UDP Flooding saldırı mimarisi Şekil 1.8'de sunulmuştur.



Şekil 1.8. UDP flooding saldırısı (UDP, 2017)

Bu tür saldırıların etkisi ‘rate limit’ (istek aşımı) yöntemi ile azaltılabilir. Çoğu işletim sistemi de ICMP cevaplarının gönderildiği adresleri bu yöntemle kısıtlayarak saldırının etkisini azaltmaktadır. Güvenlik duvarı zararlı UDP paketlerini düşürür. Böylelikle zararlı UDP paketleri hedefe ulaşmaz ve bu paketlere cevap vermesi önlenmiş olur. Linux işletim sisteminde (iptables -p udp --dport 53 -m connlimit --connlimit-above 20 --connlimit-mask 24 -j DROP) komutu ile rate limit ayarı yapılabilir.

1.1.5.2.5 DNS Amplification Saldırısı

Bu saldırı yönteminde, saldırgan hedef A kaydı için hedef kaynak IP adresine sahip bir DNS isteği gönderir. Sonrasında hedef kaynak IP adresi ile gönderilen DNS isteği yinelemeli sorgulara izin veren bir DNS sunucusuna gönderilir. Gönderilen DNS isteği 512 bayt boyutundan küçük ancak olabildiğinde büyük olması saldırının şiddetini artırmaktadır. Çünkü 512 bayt boyutundan büyük DNS sorguları UDP ile değil TCP protokolü üzerinden iletilmektedir. Saldırı esnasında kullanılacak DNS paketlerinin boyutunun olabildiğince büyük olması ise saldırının şiddetini artırmaktadır.

1.1.6. DDoS Saldırılarının Amacı

DoS, yani tek bir kaynaktan hedefe doğru saldırı yapılması şeklinde ortaya çıkan bu saldırı türü, zamanla şiddetinin ve etkisinin arttırılması için çok sayıda kaynaktan tek hedefe yapılan saldırı şekline dönüşmüştür. DoS/DDoS saldırılarında amaç, sistemin kaldırabileceği yükün çok üzerinde anlık istek ve anlık bağlantı ile sistemin yorulması, cevap veremez hale getirilmesidir. Bağlantı kapasitesinin doldurulması suretiyle yine sistemin erişilebilirliği hedef alınabilir. Ayrıca hedef sistemlerde bulunan zafiyetler de sistemin erişilebilirliği açısından risk oluşturabilir.

İşletim sistemlerinde (Windows, Linux vb.), web sunucusunda (IIS, Apache vb.), uygulama sunucusunda ya da sistemin diğer bileşenlerinde bulunan zafiyetlerden yararlanarak, sistemin işleyemeyeceği şekilde bir istek gönderildiğinde, sistemin herhangi bir bileşeninde bu isteğin işlenememesinden kaynaklanıp sistem erişilemez hale gelebilmektedir.

1.1.7. DDoS Saldırılarının Hedefleri

DDoS saldırılarının hedefi, tek bir Web sunucusundan, bir üniversiteye, bir şehrin veya bütün bir ülkenin internet bağlantısına kadar değişebilir (Kang ve ark., 2013). DDoS saldırganı aşağıdaki hedeflerden herhangi birine saldırmayı hedeflemektedir (Bhattacharyya ve Kalita, 2016):

- Yönlendiriciler (Routers)
- Bağlantılar (Links)
- Güvenlik duvarları ve savunma sistemleri (Firewalls and defense systems)
- Hedefin altyapısı (Infrastructure)
- İşletim sistemleri (Operating System)
- Uygulamalar (Applications)

1.1.8. DDoS Saldırılarının Teknik Özellikleri

DDoS saldırı algılama yöntemleri ve önleme sistemlerinin geliştirilmesi için DDoS saldırı teknik özelliklerinin anlaşılmasında fayda vardır. Bu özellikler (Koçaslan, 2015);

- Binlerce farklı kaynaklardan yapılması,
- Genellikle sahte IP adreslerin kullanılması,

- BOTNET'lerin mevcudiyeti,

- Gerçek saldırganın tespitinin imkânsızlığı,

- OSI ve TCP/IP ait katmanların neredeyse tamamını kapsayan saldırı çeşitliliğinin bulunması,

- Yoğunluk tabanlı saldırılarının, hedef sunucunun yeterli bant genişliğine sahip olmadığı durumlarda başarılı olması,

- Bant genişliği saldırılarında TCP ve HTTP Flooding saldırılarında uygulama zafiyetlerini hedef almasıdır.

Ayrıca DDoS saldırılarına maruz kalmaya sebep olan etkenler genel olarak yazılımların barındırdıkları açıklar ve protokollerin tasarımlarındaki hatalardan kaynaklanmaktadır.

1.1.9. Dünya Genelinde Yapılmış DDoS Saldırıları

DoS saldırılarının geçmişi DDoS saldırılarına nazaran daha eskiye dayanmaktadır. Sadece tek bir merkezden yapılan saldırılar çok fazla etkili olmamaktadır. Bunun yanında DDoS saldırıları 1999 yılından itibaren gündeme gelmeye başlamıştır. Resmi kayıtlara göre bilinen ilk DDoS saldırısı 1999 Ağustosunda 227 köle bilgisayar ile Minnesota Üniversitesinde gerçekleşmiştir (Garber, 2000).

Bu saldırıdan sonra 2000 yılında Amazon, Yahoo, eBay ve Datek şirketlerine DDoS saldırıları gerçekleştirilmiştir. Bu saldırılarda Yahoo, üç saat boyunca kullanıcılara hizmet verememiştir. Şubat 2001 de İrlanda Ekonomi Bakanlığı sunucularına yapılan saldırıda sunucular büyük ölçüde zarar görmüştür (Wikipedia, 2017).

2002’de DNS Root Server’lara yapılan saldırı sonucunda 13 sunucudan dokuzu büyük ölçüde zarar görmüştür. 2007’de Wolfenstain, Counter Strike gibi oyunlarında aralarında bulunduğu on binden fazla oyun sunucusuna binden fazla bilgisayardan oluşan bir BOTNET ağıyla saldırı düzenlenmiş ve birçok bilgi ifşa olmuştur. 2008’de Gürcistan Cumhurbaşkanlığı, Ulusal Bankası ve birçok devlet sitesi Rus korsanlarının DDoS saldırılarına maruz kalmıştır. 2010 yılında Mavimarmara ve Wikileaks olaylarını protesto etmek için yapılan saldırılar ve 2011 yılında PlayStation sunucularına yapılan DDoS saldırıları en dikkat çeken saldırılardır. 2012 yılında ABD Finans kuruluşlarına karşı çok ciddi DDoS atakları gerçekleştirilmiştir. Bu saldırılarda PHP tabanlı web uygulamaları kullanılmıştır. 2012-2015 yıllarında yapılan saldırılar incelendiğinde bu saldırıların özellikle finans sektörünü hedef aldığı görülmektedir (Wikipedia, 2017).

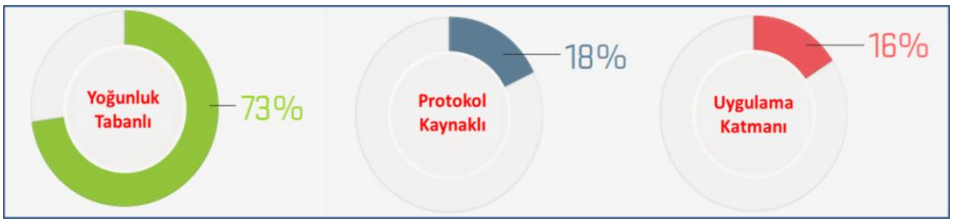
Neredeyse her gün yeni bir çeşidi ve formu geliştirilen DDoS saldırılarının 18 yılda 100 kat artması ile 1 Tbps'de gibi bir devasa boyuta ulaşmıştır. Bununla birlikte DDoS saldırısının ilk ortaya çıktığı zamandan beri gösterdiği çeşitlilik ve sürekli evrimleşmesi endişe vericidir.

1.1.10. DDoS Saldırı Şiddeti

DDoS saldırı çeşitliliği önemli derecede değişirken, siber suçlular alınan güvenlik önlemlerini atlatmak ve hedeflerine ulaşmak için kullandıkları yöntemleri sürekli geliştirmektedir.

Son 10 yılda yapılan saldırılar baz alındığında, yoğunluk tabanlı saldırıların 2016 yılında da saldırı şiddeti açısından ilk basamakta olduğu görülmektedir. Son iki yılda, dünyadaki hacimsel saldırıların ölçeği ve sıklığında önemli bir artış olduğunu açıktır. Hacimsel nitelikteki saldırıların oranı 2015 yıllında yüzde 65 iken 2016

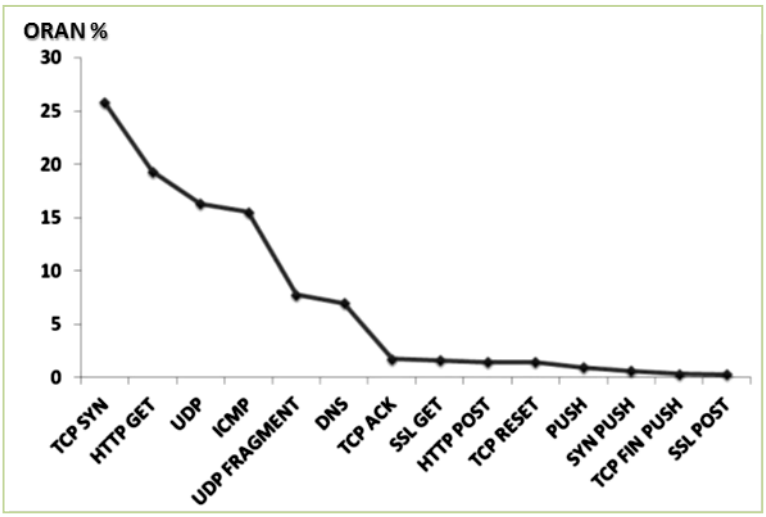
yılında yüzde 73'e yükselmiştir. Şekil 1.9'da görüldüğü gibi uygulama katmanını hedef alan saldırıların oranı 2016 yılında geçen yıllara nazaran durağan kalmıştır.



Şekil 1.9. 2016 Yılında yapılan DDoS saldırı çeşitlerine ait istatistikler (Arbor, 2017)

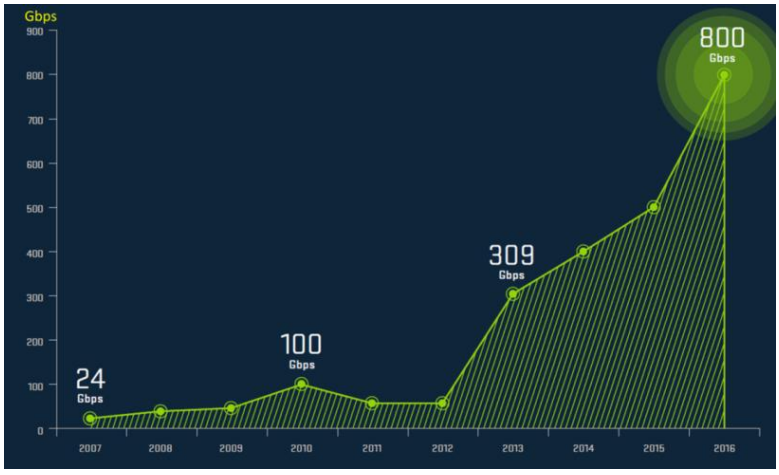
Güvenlik sistemleri, TV, tıbbi cihaz, GPS ve akıllı saatler vb. çeşitli özelliklere sahip elektronik nesneleri birbirine bağlamak temel fikri olan Nesnelerin İnterneti (IoT) olarak adlandırılan bir ağ senaryosu 2015 yılından itibaren kullanımı yaygınlaşmıştır. Bu ağ senaryosuna; sensörler, avuç içi cihazlar, hava gözlemleri, santrallerdeki kontrol valfleri, hapishanelerdeki kapı kilitleri, trafik işaretleri gibi birçok hizmetin daha bağlanması, saldırganlar için daha fazla fırsat doğurmasına sebebiyet vermektedir. Çünkü bunların çoğu az güvenlik mekanizmaları ile donatılmış olması ve güncellenmelerinin ertelenmesi sebebiyle saldırganların köle olarak kullanımına yeni bir aday cihaz yelpazesini çevirmektedir (Atzori ve ark., 2010).

2016 yılına kadar olan DDoS saldırı istatistikleri Şekil 1.10'da gösterilmektedir. X ekseni üzerinde yaygın olarak kullanılan DDoS saldırıları arasında TCP SYN, HTTP GET, UDP ve ICMP Flooding en çok tercih edilen saldırı çeşididir.



Şekil 1.10. 2016 yılında yapılan DDoS saldırı türleri

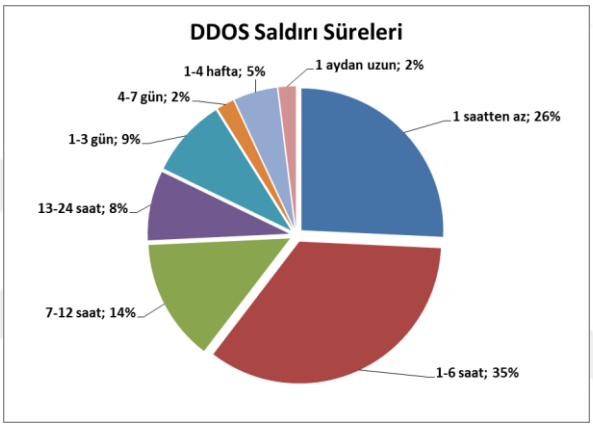
2016 yılında yapılan araştırmalarda; saldırganlar, saldırıların boyutunu en üst düzeye çıkarmak için DNS, NTP, SSDP, Chargen ve diğer protokollerdeki güvenlik açıklarından faydalanmak için yansıtma/yükseltme (reflection/amplification) tekniklerini kullanmaya devam etmişlerdir. 2016 yılından itibaren yansıtma/ yükseltme teknikleri olmaksızın büyük yoğunlukta saldırı üretmek için IoT cihazlarının kullanımında belirgin bir artış olmuştur. 2016 yılında bildirilen en büyük saldırı 800 Gbps'dir, 2012 yılından itibaren yoğunluğun büyük derecede arttığı Şekil 1.11'de görülmektedir.



Şekil 1.11. Son 10 yılda yapılan DDoS saldırı istatistikleri (Arbor, 2017).

1.1.11. DDoS Saldırı Süresi

DDoS saldırılarıyla ilgili son istatistiklerde (Şekil 1.11) görüldüğü gibi saldırı şiddeti ve sıklığının yıldan yıla arttığını görülmektedir. 2016 yılında gerçekleştirilen DDoS saldırı süreleri Şekil 1.12'de sunulmuştur. Bu saldırı süreleri incelendiğinde saldırıların büyük bölümü 1-6 saat arasında yapıldığı görülmektedir. Bu sürenin hizmet kalitesinden ödün vermeden devamlılığı için uzun bir süre olduğu değerlendirilmektedir.



Şekil 1.12. 2016 yılına ait DDoS saldırı süreleri (Arbor, 2017).

1.2. Köle Bilgisayar

İnternet teknolojilerindeki hızlı gelişmelere paralel olarak siber saldırganların teknikleri ve profesyonellikleri katlanarak artmaktadır. DDoS saldırılarına maruz kalan sistemin yanında ikincil kurbanlar; zararlı yazılım bulaştırılmış bilgisayar, akıllı telefon, IP kamera, IoT ve internete bağlı cihazlardır.

Temel olarak tek bir IP adresinden yani sistemden gelen saldırılar donanımsal ya da yazılımsal olarak önlenebilir. Fakat birden fazla noktadan gelen saldırıları

tespit etmek ve engellemek oldukça zordur. DDoS saldırılarında amaç sistemleri işlevsiz hale getirmek ve kullanımlarını engellemektir. DDoS saldırıları gerçekleştirmek için saldırganlar tarafından kullanılan bilgisayarlar köle (zombi) bilgisayar olarak adlandırılmaktadır. Köle bilgisayar toplulukları ise "BOTNET" olarak isimlendirilir. Saldırganlar birçok köle bilgisayarı tek bir hedefe yönlendirebilirler. BOTNET saldırıları; DDoS saldırıları yapmak, istenmeyen e-posta mesajları göndermek ve virüsleri yaymak gibi amaçlar için kullanılırlar.

Köle bilgisayarlar zararlı yazılım geliştiricisi olan BOTMASTER tarafından yönetilmektedir. Kontrol edilen bu bilgisayarlar saldırganların doğrudan yönetimi ile değil, ara bir segment kullanılarak kendilerini çok rahatlıkla gizleyebilmektedir. Bu kontrol merkezleri Komuta ve Kontrol (C&C) Sunucuları" olarak adlandırılmaktadır. BOTNET mimarisinde BOT'lar P2P, IRC, HTTP veya DNS tabanlı C&C sistemi kullanılarak kontrol edilir. Geliştirilen bu yapı ile hedef alınan sunucu, web sayfası veya internet servis sağlayıcı dünyanın farklı yerlerindeki BOTNET'in bir parçası olmuş bilgisayar tarafından saldırıya maruz kalmaktadır. Köle bilgisayarlar bu yapının içinde olduğunun farkında değildir, ancak bilgisayarının durduk yere yavaşlaması, internet bağlantısının sürekli paket gönderildiğinden internet hızının yavaşlamasıyla kullanıcılar bunun farkına varabilir veya iyi bir anti-virüs ile kendi bilgisayarlarını incelediklerinde bu durumdan kurtulabilmektedirler.

BOTNET ve DDoS saldırıları arasında doğrudan bir ilişki vardır. Tek bir IP'den yapılan saldırı çok çabuk ve basit bir şekilde IP adresinin yasaklanmasıyla engellenebilir. Ama bunun yüzbinlerce ve dünyanın çeşitli yerlerinden yapılan bir BOTNET saldırısı olarak ortaya çıktığında, alınan emniyet tedbirlerinin çok güçlü olmadığı durumlarda saldırının amacına ulaşması anlamına gelmektedir. Amaçlanan servis dışı bırakma işlemi gerçekleşmiş olur. Siber silahın bir parçası olan DDoS ancak BOTNET ordusundaki BOT'ların sayısı ve çeşitliliği (PC, Akıllı Cihaz, IP Kamera, IoT vb.) ile güçlenmektedir. Yakın geçmişte, çeşitli BOTNET'ler ortaya çıkmıştır. Bunların bazıları Agobot, Spybot, RBot ve SDBot'tur.

Yakın geçmişte, BOTNET teknolojisi oldukça ileri düzey tekniklerle gelişmiştir. BOTNET teknolojisinin gelişimi ve DDoS saldırısı üretimi bağlamındaki özellikleri, Geleneksel BOTNET ve Mobil BOTNET'ler olmak üzere iki kategoride ele alınmaktadır.

1.2.1. Geleneksel BOTNET'ler İle Yapılan DDoS Saldırıları

Büyük ölçekli ve gelişmiş DDoS saldırıları BOTNET teknolojisi kullanılarak yapılmaktadır. DDoS saldırısında BOTNET teknolojisinin kullanılmasındaki ana sebep, çeşitli DDoS saldırıları türlerinin üretilmesini sağlayan büyüme kapasitesi ve esnekliğin olmasıdır. Saldırganların bu teknolojiyi tercih etmesinin dört önemli nedeni;

a) Kısa sürede yüksek yoğunluklu bir saldırı başlatmak için çok sayıda köle bilgisayarın bulunması,

b) Güvenlik mekanizmalarını atlamak için protokol açıklıklarının bulunması,

c) Saldırı kaynağının belirlenmesindeki zorluk,

d) Ayırt edici özelliklerin olmaması nedeniyle zararlı yazılım trafiği ile (özellikle düşük hızlı DDoS saldırıları) meşru trafiğin gerçek zamanlı olarak ayrıştırılmasındaki zorluklardır. Internet Relay Chat (IRC) sisteminin geliştirilmesindeki maksat; idari destek, basit oyunlar ve sohbet etmek için metin türü mesajlaşma ile hizmet sağlamaktır. Ancak DDoS saldırılarını başlatılmasında IRC sistemi kullanılmaktadır. BOTNET tabanlı bir DDoS saldırısı başlatılmasında aşağıda sunulan üç temel modelden herhangi biri veya kombinasyonu kullanır;

a) Arabirim modeli (Agent Handler Model),
b) IRC tabanlı modeli (IRC-Based Model),
c) Web tabanlı model (Web-Based Model)’dir

1.2.1.1. Arabirim Modeli

DDoS saldırısının başarılı bir şekilde başlatılması için dört aşamada işletilir. Bunlar saldırgan, arabirim, köle bilgisayarlar ve hedeftir. Saldırgan tarafından DDoS saldırıları başlatmak için C&C sunucusu kullanma amacı, saldırganın tespitinde kullanılan IP geri izleme olasılığının üstesinden gelmektir. Köle bilgisayarlar saldırıyı gerçekleştirmekten sorumludur. Saldırgan TCP, UDP veya ICMP gibi protokollerin zayıf noktalarını istismar ederek saldırıyı başlatmaktadır.

1.2.1.2. IRC Tabanlı Model

Metin tabanlı bir sohbet sistemi olan IRC farkında olmadan BOTNET'lerin gelişimini sağlamıştır. IRC tabanlı DDoS saldırıları, anlık büyük ölçekli saldırı trafiğine ulaşması özelliği nedeniyle çok yaygın olarak kullanılmaktadır. Başarılı bir kurulumdan sonra, sistem ve bilgisayar arasında IRC sunucusu bir arka kapı genellikle mevcuttur; bu arka kapı saldırgan tarafından kontrol edilir. Saldırgan, IRC sayesinde DDoS saldırısını başlatır, kimlik doğrulamasını yapar ve (komutlar vererek) bir anda birçok köle bilgisayarı yönlendirebilir. IRC tabanlı saldırılar farklı birçok yazılım kodu çeşitlemesi ve protokolü içerebilir. Arabirim tabanlı DDoS saldırıları gibi IRC tabanlı bir DDoS saldırısı TCP, ICMP veya UDP protokollerini kullanır.

1.2.1.3. Web Tabanlı Model

Web tabanlı modeller BOTNET komutu ve kontrolü için etkili bir alternatiflerdir. Bu model, sadece bir web sitesinden istatistik toplamaya yardımcı olmakla kalmaz, aynı zamanda gelişmiş PHP kodları aracılığıyla şifreli iletişim

sağlamaktadır. IRC'ye kıyasla, web tabanlı model; kontrol, kurulum, gelişmiş raporlama araçları ile kullanıcı dostu ara yüze sahip olması, trafiği gizleme kolaylığı, 80 portunu kullanılması nedeniyle filtrelemede zorluk ve düşük bant kullanımı nedeniyle daha üstündür.

Sonuç olarak, DDoS saldırıları kaynaklarının tespitinin yanı sıra TCP 80 portu üzerinden bu tür trafiğin filtrelenmesi son derece zordur. Ayrıca, saldırganlar sürekli olarak DDoS saldırılarını daha etkili hale getirmek için BOTNET teknolojisini geliştirmeye devam etmektedir.

1.2.1.4. Geleneksel BOTNET Örnekleri

Son zamanlardaki en gelişmiş DDoS saldırıları, BOTNET teknolojisi kullanılarak yapılanlardır. Son birkaç yılda, BOTNET teknolojisinde birçok önemli gelişme ortaya çıktı. Çeşitli saldırı türlerini yapmak için sıkça kullanılan birkaç BOT örnekleri;

a) **Bagle**: 2004 yılında tanıtılan PROXY-to-relay e-posta SPAM'lerinde kullanılabilir. Bagle'ye dahil bilgisayar sayısı 280.000 civarındadır. Bir günde 8.31 milyar SPAM e-postayı gönderme gücüne sahiptir.

b) **Nugache**: Truva internet solucanının özelleştirmesi ile tasarlanmıştır. Herhangi bir C & C sunucusu olmaksızın P2P iletişimine izin verir ve bu da kolaylıkla algılanamayacak hale gelmesini sağlar. Bu durumda BOTNET için yeni bir esneklik düzeyi sunmaktadır.

c) **Rustock:** Bu BOT, istenmeyen e-postalarının (SPAM) dağıtımına yardımcı olan bir arka kapı (Truva) türüdür. Rustock, virüs bulaşmış bir makineden saatte 25.000'den fazla SPAM mesajı gönderebilir. Rustock, 470.000 ila 690.000 ele geçirilmiş bilgisayar ile 13.82 milyar günlük SPAM eposta üretebilmektedir.

d) **MegaD**: MegaD, 2007'de tanımlanan SPAM BOTNET'idir. 500.000 üyesi vardır.

e) **Srizbi**: Srizbi, Truva Atı yoluyla bulaşan bir virüs sayesinde köle bilgisayarlar üretir. DDoS maksatlı kullanılan 400.000 köle bilgisayarı bulunmaktadır.

f) **Conficker**: Bu güçlü ve etkileyici bilgisayar solucanı milyonlarca kullanıcıyı anında bulaşabilmektedir. Windows işletim sisteminin zayıf noktalarını istismar edebilen ve BOTNET oluşturmak için yönetici şifrelerini çalma kapasitesine sahiptir. Savunulması zor bir internet solucan türüne sahiptir. 10 milyondan fazla ele geçirilmiş köle bilgisayarı vardır.

g) **Bobax**: C&C sunucusu ile iletişim için düz metin HTTP kullanır. Bu solucan Windows sistemlerinde DCOM ve LSASS güvenlik açıklarını kullanmaktadır. 185.000 civarında üyesi bulunmaktadır.

h) **Kraken**: Virüs bulaşmış bir bilgisayardan SPAM epostaları yaymak için kullanılır. C&C ile şifrelenmiş mesajlar kullanarak iletişim kurar ve TCP ve UDP protokolleriyle iletişim kurabilir. 400.000 civarında üye bilgisayarı vardır.

i) **Waledac:** İndirilebilen karmaşık bir solucan türüne sahiptir. Ağ PROXY'si olarak davranabilir, SPAM epostalar gönderebilir, virüs bulaşmış bilgisayarları e-posta adresleri ve parolalarını elde edebilir ve DoS saldırısı başlatabilir. Sosyal mühendislik tarafındaki zayıf noktaları kullanarak yayılım sağlar.

j) **Donbot**: SPAM e-postaları göndermek için özel olarak tasarlanmış bir BOTNET'dur. Yaklaşık 125.000 bilgisayarı ile günde 800 milyon SPAM eposta gönderebilmektedir.

1.2.2. Mobile BOTNET'ler ile Yapılan DDoS Saldırıları

Mobil BOTNET geleneksel BOTNET yapısına benzemektedir. Bu yapıda da BOTMASTER tarafından C&C sunucusu vasıtasıyla uzaktan kontrol edilen, zararlı yazılım yüklenmiş akıllı cihazlar DDoS maksadıyla kullanılmaktadır. Mobil BOTNET yönetiminde üç çeşit C & C sunucusu kullanılmaktadır;

a) GSM tabanlı (SMS) C&C,

b) İnternet tabanlı (IP) C&C,

c) Yerel kablosuz C&C mekanizmasıdır.

1.2.2.1. Mobil BOTNET Saldırıları Özellikleri

Öncelikle BOTNET işlevselliğinin ortaya konulması için ortak özellikleri belirlenmeli ve bu özellikler sayesinde olası diğer BOTNET saldırılarının tespitinde bu husus değerlendirilmelidir. Bu çalışmada BOTNET saldırılarının ortak özelliklerini belirlemek için, son yıllarda yaygın ve çok aktif olan ZtorgB.Gen, Lop.c, Muetan.b, Zitmo, TigerBot, AnServerBot, Geinimi, PjApps, RootSmart/Bmaster, DroidDream, DroidKungFu, SMSpacem, FakePlayer, ADRD, Spy.Banker.HU, BaseBridge ve Nickispy BOTNET saldırıları incelenmiştir (Spreitzenbarth, 2017). Bu çalışmada analiz edilen MALWARE örnekleri Contagio Kütüphanesinden (Araştırma amaçlarıyla paylaşılan bir MALWARE Kütüphanesi) indirilmiştir. BOTNET saldırıları arasındaki ortak özellikleri belirlemek için izin tabanlı filtreleme yaklaşımı kullanılmıştır. Bunun sonucunda tespit edilen ortak özellikler (Şekil 1,13); zararlı yazılım paketlenmesi, uzaktan yönetim, e-posta ve SMS Okuma-Gönderme, veri hırsızlığı, ek içerik indirme/kurma, kök klasör (Root) saldırısı, üçüncü parti uygulama mağazaları ve uygulama izinleridir.

Sıra Numarası		Ztorg.B.Gen	lop.c	Muetan.b	Zitmo	TigerBot	AnserverBot	Geinimi	PjApps	DroidDream	RootSmart/ Bmaster	DroidKungFu	SMSpacem	FakePlayer	ADRD	Spy.Banker.HU	BaseBridge	NickiSpy
1	Zararlı Yazılım Paketlenmesi/indirme		+	+		+			+	+		+			+			
2	Uzaktan Yönetim	+	+	+		+	+	+	+	+	+	+			+		+	+
3	E-posta ve SMS Okuma-Gönderme	+			+			+	+		+			+		+		
4	Veri Hırsızlığı	+		+	+	+	+	+	+	+	+	+	+		+		+	+
5	Ek İçerik İndirme/Kurma		+					+	+	+	+							
6	Kök Klasör (Root) saldırısı		+			+				+	+	+						
7	Üçüncü Parti Uygulama Mağazaları	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
8	Uygulama İzinleri	+				+												
Diğer	Mobil Bankacılık Saldırısı				+													
	Telefon Araması Yapma							+										
	IMEI Hırsızlığı											+			+			
	SMS ile HTTP Bağlantısı Gönderme												+					

Şekil 1.13. Zararlı yazılım özelikleri

Belirlenen bu ortak özelliklerin BOTNET temel özellikleri olarak nasıl kullanıldığı örnekleri ile açıklanmıştır.

1.2.2.1.1. Zararlı Yazılımın Paketlenmesi

ANDROID ve iOS işletim sistemleri gibi tüm mobil işletim sistemleri kullanıcılarına resmi uygulama mağazalarından (Google Play Store, Samsung Apps ve Apple Store) uygulamaları indirme hizmeti sağlamaktadır. Ancak ANDROID işletim sistemi resmi olmayan uygulama mağazaları ve sunuculardan da uygulama kurulmasına izin vermektedir. BOTNET saldırılarının yönetimi zararlı yazılım kodları içeren uygulamalar ile yapılmaktadır. Bu kodlar, orijinal uygulamada ters mühendislik işlemi yapıldıktan sonra orijinal uygulama koduna zararlı yazılım kodunun ilave edilerek yeniden paketlenir ve kullanıma sunulur. Bu husus BOTNET saldırılarının dağıtımında kullanılan en yaygın yöntemdir. "PjApps", geleneksel BOTNET işlevselliğine sahip zararlı yazılım kod örneklerinden biridir. PjApps ilave edilmiş yazılım, içinde bulunduğu cihaza bir arka kapı (Backdoor) açılmasına izin verir ve bu izinle uzaktaki sunucudan komut alınması sağlanır (Castillo, 2016).

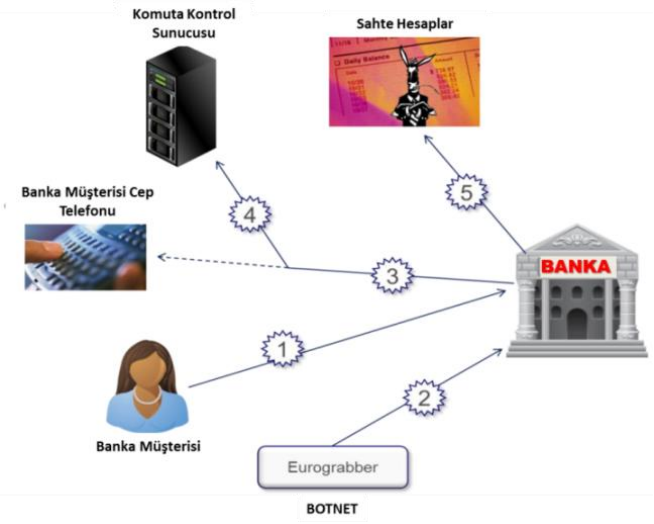
1.2.2.1.2. Uzaktan Yönetim

BOTNET saldırılarının en önemli özelliklerinden birisi; uzaktaki bir sunucudan komutlar alabilmesidir. “BOTMASTER” komutlarını hedef cihazlara göndermek ve yanıt almak için C&C sunucu ara yüzünü kullanır (Eslahi ve ark., 2012). Mobil BOTNET saldırılarda kullanılan güncel teknikler ile geleneksel teknikler çok benzerdir. İlk seçenek, komutları doğrudan C&C sunucusundan BOT'a göndermektir. Diğer seçenek, BOT’un düzenli aralıklarla C&C sunucusuyla iletişime geçmesine izin vermek ve yeni komutların mevcut olup olmadığını sormasıdır.

"AnserverBot" bu türde bir mobil BOTNET saldırısıdır. AnserverBot, virüs bulaşmış cihazdaki güvenlik çözümünü tespit etme ve devre dışı bırakmanın yanı sıra, kendini her türlü değişiklikten korumak için bütünlüğünü doğrulama imzasını kontrol eder. "TigerBot", web teknolojisi yerine SMS ile kontrol edilen bir BOT'tur. C&C mesajlarını algılar ve onları mobil cihaz sahiplerinden gizler. SMS mesajları gibi özel veriler toplamak yerine, telefon görüşmelerini ve telefon görüşmesi olmadığı zamanlarda ortamdaki sesleri kaydeder. Şekil 1.13'de bulunan ikinci özelliğe sahip diğer BOT'larda AdserverBOT ve TigerBot gibi uzakta bulunan bir C&C sunucusu tarafından yönetilebilmektedir.

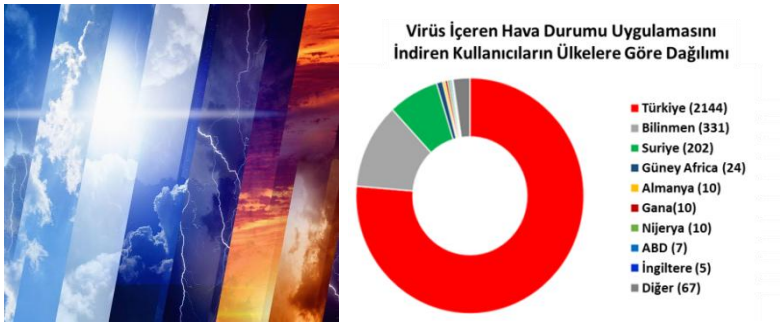
1.2.2.1.3. E-posta ve SMS Okuma-Gönderme

Geleneksel BOTNET saldırısının temel amacı mali kazanç sağlamaktır. Belirli bir hizmete yönelik kullanılan telefon numaralarından oluşan ve normal telefon hatlarına nazaran yüksek ücret tarifesi sahip ücretli hatlara düzenli aralıklarla gizlice SMS gönderen BOTNET, önemli miktarda maliyetlere neden olabilir. "RootSmart/Bmaster" ücretli hatlara SMS göndererek milyonlarca dolar kazanmıştır. Diğer bir zararlı yazılım olan "Zitmo"; Symbian, Windows Mobile, BlackBerry ve ANDROID gibi farklı mobil işletim sistemlerini etkileyen bir BOT'dur. Bu zararlı yazılım bankaların, Kimlik Doğrulama Mesajı (TAC) içindeki verilen tek kullanımlık SMS şifresini çalmak suretiyle müşterilerin bankacılık işlemlerine ulaşmaktadır. Bu yöntemle Avrupa'daki bankalardan 2012 yılında 36 Milyon Euro çalınmıştır (Techworld, 2017). Zararlı yazılım hırsızlık yöntemi Şekil 1.14'de gösterilmiştir.



Şekil 1.14. Zitmo zararlı yazılımı çalışma yöntemi (Techworld, 2017).

ESET güvenlik firması tarafından Şubat 2017'de "Spy.Banker.HU" adıyla etiketlenen bu truva atı, yaygın olarak kullanılan hava durumu uygulaması "Good Weather"ın zararlı hale dönüştürmüş ve 22 Türk Banka müşterisini hedef alan bir virüstür. Uygulama mağazası Google Play Store üzerinden indirilebilen bu uygulamanın iki sürümü tespit edilmiştir. ESET'in uyarısı üzerine uygulamalar Google Play'den kaldırılmıştır. Zararlı yazılım, uygulama mağazasında kısa süre yer almasına rağmen kullanıcılar tarafından binlerce kez indirilmiştir. İlk tespitlere göre 48 ülkede 5 bin kullanıcıya ulaşılmıştır (Şekil 1.15). Uygulama kullanıcı tarafından yüklendikten sonra hava durumu görünümlü ikon önce kayboluyor. Etkilenen cihazın ekranında, kullanıcıdan yönetici haklarını talep eden bir mesaj görünmektedir. Kullanıcı bu mesajı onaylayarak zararlı yazılıma kilit ekranı parolasını değiştirme ve ekranı kilitleme yetkisi vermiş olmaktadır. Bu yetkilerle birlikte SMS mesajlarına da ulaşabilme imkânı alan zararlı uygulamanın önünde hiçbir engel kalmamaktadır. Kullanıcılar ekranlarına güzel bir hava durumu uygulaması eklediklerini düşünürken arka planda çalışan zararlı uygulama, cihazdan edindiği SMS mesajları ve bankacılık bilgileri gibi cihazın sahibine ait verileri, zararlı yazılımın barındığı C&C sunucularına, dolayısıyla da siber hırsızlara iletmektedir (Welivesecurity, 2017).



Şekil 1.15. Virüs içeren hava durumu uygulaması kullanıcı durumu (Welivesecurity, 2017).

1.2.2.1.4. Veri Hırsızlığı

BOTNET saldırganları, elde ettikleri kişisel verileri uzaktaki bir sunucuya gönderirler. Bu husus zararlı uygulamanın cihaza kurulumundan sonra gerçekleşir. BOTNET saldırıları genellikle şu bilgileri elde etmek isterler: IMEI (Uluslararası Mobil Cihaz Kimliği) numarası, GPS konum bilgisi, telefon rehberi, cihaz modeli ve seri numarası, görüşme kayıtları, yüklü uygulamalar, e-posta bilgileri, tarayıcı geçmişleri ve fotoğraflardır. "Geinimi", geleneksel BOTNET işlevlerini sergileyen zararlı bir yazılımdır (Thakkar, 2015). Bu zararlı yazılım, cihazdaki kişisel verileri toplar ve bu bilgiyi uzaktaki bir sunucuya iletir. "PjApps.A", IMEI, telefon numarası ve SMS bilgilerini toplar aynı şekilde uzaktaki bir sunucuya gönderir. "TigerBot.A" de benzer bir zararlı yazılımdır. BOTNET saldırılarının bir diğer temel özelliği Coğrafi Konum Sistem (GPS) bilgisini elde etmektir. Konum bilgisi cep telefonu kullanıcılar için çok önemli bir kişisel veri olmasına rağmen, zararlı yazılımlar tarafından elde edilebilmektedir. Cep telefonlarındaki konum bilgilerinin gizliliğine ilişkin kapsamlı araştırma (Minch, 2004)'de sunulmuştur.

1.2.2.1.5. Ek İçerik İndirme/Kurma

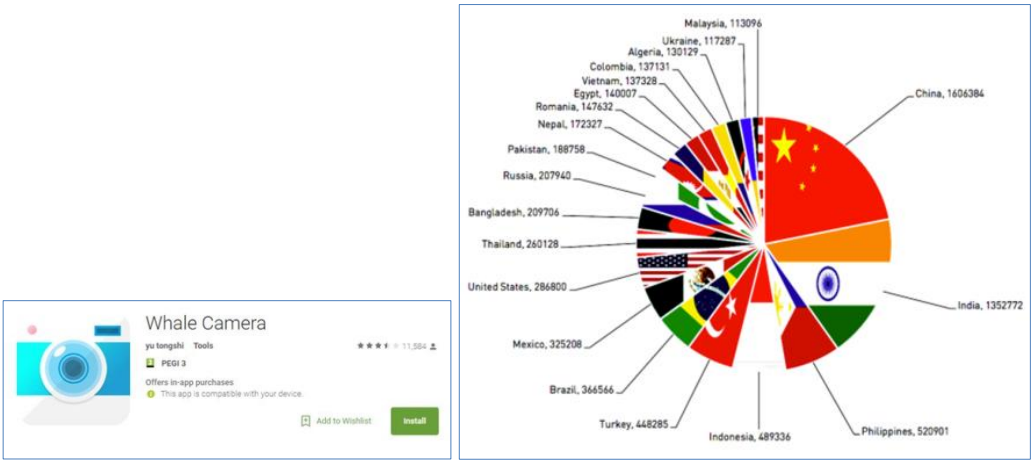
Mobil BOTNET saldırılarının en yeni özelliklerinden birisi zararlı yazılım bulaşmış akıllı telefonlarda, kullanıcının bilgisi dışında cihazlara ek içerik

indirilebilmesidir. Bu içerik, genelde zararlı yazılım kodları ile ilgili olup, BOTNET saldırısının cihaz içindeki hareket kabiliyetini artırır ve geliştirir. Bu içerikler kullanıcının yanlış yönlendirilmesi ile gerekli indirme işlemini yapması veya bilgisi olmadan indirilmesi sağlanır. "DroidDream" zararlı yazılımı, virüs bulaşmış cihaza başka bir uygulama daha indirerek hareket kabiliyetini genişletmektedir. Yeni indirilen bu uygulama sayesinde kullanıcı "DroidDream" zararlı yazılımını cihazdan kaldıramaz veya silemez.

1.2.2.1.6. Kök Klasör (Root) Saldırısı

Mobil telefon kullanıcılarının bir kısmı orijinal telefon yazılımı dışında işletim sisteminde daha fazla hareket kabiliyeti ve yazılım yetkisi elde edebilmek için ROOT yetkisi üzerinde değişiklik yapmaktadır. Buna karşın, ROOT yetkisi olan cihazlarda mobil BOTNET kendisine yeni imkânlar yaratabilir. "RootSmart/Bmaster" zararlı yazılımı, bazı ANDROID işletim sistemi sürümlerinde kendisi ROOT erişimi elde etme olanağına sahiptir. "DroidDream", 2011 yılında Google Play Store'da 50'den fazla uygulamaya bulaşarak, kullanıcı telefonlarına ulaşmıştır. Bu sayede, bulaştığı 200.000 kullanıcıyı ile güçlü bir BOTNET oluşturma hedefindedir (Zeng, 2012).

Check Point firması, Google Play'deki 20'den fazla uygulamada gizli olan HummingBad zararlı yazılımının yeni bir çeşidini buldu. Virüsten etkilenen bu uygulamaları, hiçbir şeyden haberi olamayan kullanıcılar tarafından milyonlarca kez indirildi (Checkpoint, 2017). Check Point firması Kasım 2016 tarihinde söz konusu zararlı yazılımı Google Play'den kaldırılması için Google Güvenlik ekibine bildirmesine rağmen, 10 milyondan fazla cihazın bu virüsten etkilendiği değerlendirilmektedir (Şekil 1.16) (Arstechnica, 2017).



Şekil 1.16. Virüs içeren uygulamaların kullanıcı durumu (Arstechnica, 2017).

1.2.2.1.7. Üçüncü Parti Uygulama Mağazaları

Google Play Store, ANDROID Market ve BlackBerry App World gibi resmi mağazalar uygulama indirmenin en temel yöntemidir. ANDROID kullanıcılarının telefonlarındaki resmi mağazalara ek olarak üçüncü parti uygulama mağazaları veya forum sitelerinden uygulamalar ücretli veya ücretsiz elde edebilmektedir. Bu üçüncü parti uygulama mağazaları, resmi uygulama mağazalarında bulunmayan benzersiz birçok özellik sunmaktadır. Örneğin, birçok ücretli veya reklam içerikli uygulamaları ücretsiz olarak sunmakta, deneme süresi olan uygulamalar sınırsız kullanım süresine sahip olmasına rağmen, bu uygulamaların birçoğu zararlı yazılım içermektedir.

1.2.2.1.8. Uygulama İzinleri

ANDROID uygulaması, hassas kaynak ve işlemlere erişimi denetleyen izinler ile tanımlar. ANDROID işletim sisteminde 137 adet tanımlı izin vardır (ANDROID, 2017), bunların arasında 122 adet izin üçüncü parti uygulamaları için kullanılabilmektedir (Au ve ark., 2011). İzinler, ANDROID işletim sisteminde

AndroidManifest.xml dosyasında tanımlanmaktadır. ANDROID bu izinleri yüklenen uygulamaların güvenlik riskleri hakkında kullanıcıları bilgilendirmek için kullanılır (Khalo, 2016). Fakat araştırmacılar, ANDROID izin bildirimlerinin çoğunlukla kullanıcılar tarafından göz ardı edildiği veya hiç dikkate alınmadan uygulamaların kurulduğunu analiz etmiştir (Felt ve ark., 2012; Enck ve ark., 2009).

Örneğin, hava durumu bilgisini almak için yüklenen basit bir uygulama, telefonumuzdaki birçok yetkiye (Kamera, GPS, mikrofon, rehber, hafıza erişimi vb.) sahip olabilmektedir. Bu uygulama yetkilerinin kullanıcılar tarafından düzenlenmesi ANDROID 6.0 Marshmallow sürümü ve sonrasında geliştirilmiştir. Daha önceki sürümlerde bu yetki kullanıcılara verilmemiştir. Aşağıda sunulan tabloda görüldüğü gibi kullanıcıların %65.9 (Şekil 1.17) gibi büyük bir bölümü kullandığı uygulama yetkilerini düzenleyemeye yetkisi bulunmamaktadır. Bu durum ise zararlı yazılım içiren uygulama geliştiricileri tarafından kullanılmaktadır.

Sürüm Numarası	Android Sürümü	Kullanım Oranı	Uygulama Yetki Kısıtlama
2.3.3	Gingerbread	1.0%	Yok
4.0.3	Ice Cream Sandwich	1.0%	
4.0.4			
4.1.x	Jelly Bean	3.7%	
4.2.x		5.4%	
4.3		1.5%	
4.4	KitKat	20.8%	
5.0	Lollipop	9.4%	
5.1		23.1%	
6.0	**Marshmallow**	**31.3%**	**Var**
7.0	**Nougat**	**2.4%**	
7.1		**0.4%**	

Şekil 1.17. ANDROID işletim sistemi sürüm kullanım oranları (Android, 2017).

Yukarıda anlatılan BOTNET özellikleri sayesinde yapılabilecek saldırılar hakkında fikir sahibi olunmaktadır. Zararlı yazılımın neden bir bilgisayara veya akıllı cihaza erişmek ve yayılma politikasının olduğu bu özellikler sayesinde ortaya çıkmaktadır. Tek bir IP'den yapılan saldırı çok çabuk ve basit bir şekilde IP adresi

yasaklanarak engellenebilir. Ama bunun yüzbinlerce ve dünyanın çeşitli yerlerinden yapılan bir saldırı olarak ortaya çıktığında, alınan emniyet tedbirlerinin çok güçlü olmadığı durumlarda saldırı amacına ulaşmaktadır. Amaçlanan servis dışı bırakma işlemi gerçekleşmiş olur. Siber silahın bir parçası olan DDoS ancak BOTNET ordusundaki BOT'ların sayısı ve çeşitliliği (PC, Akıllı Cihaz, IP Kamera, IoT vb.) ile güçlenmektedir. Şekil 1.13'de anlatılın özelliklerden en önemli olanları ve BOTNET temel özelliklerini yansıtan; uzaktan yönetim, zararlı yazılım paketlenmesi, uygulama izinler ve üçüncü parti uygulama mağazalarından yayılmadır. Uygulama izinleri ve uzaktan yönetim sayesinde C&C sunucusundan aldığı komutlar doğrultusunda saldırı yapılacak hedefe istek gönderme ve sonlandırma zamanı öğrenilmektedir. BOT sayısı ne kadar çok olursa BOTNET ile yapılacak DDoS saldırısı o kadar etkili ve güçlü olmaktadır. Zararlı yazılım bulaşmış olması uygulama safhasının başladığı anlamına gelmemektedir. Kişisel veri, SMS ve epostalarının üçüncü kişilerin eline geçmesini engellemek ve BOTNET'in bir parçası olmamak için üçüncü parti uygulama mağazalarından uygulama yüklerken çok dikkatli olunmalı ve iyi bir anti-virüs yazılımına sahip olmak gerekmektedir. İşletim sistemi Android 6.0 ve sonrasına sahip cihazlarda uygulama izinlerinin mutlaka kontrol edilerek; uygulamalardaki gereğinden ve amacı dışında verilen izinlerin kaldırılması çok önemlidir. Örneğin bir hava durumu uygulaması için mikrofon ve kamera izinlerine ihtiyaç duyulmazken, veri kullanımı ve konum bilgisi izinlerinin verilmesi gerekliliktir.

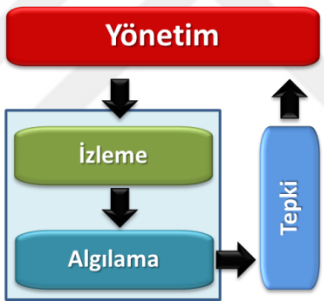
1.3. DDoS ve BOTNET Saldırılarını Algılama Sistemi

Teknolojinin gelişimi ile bilgisayar ve internet kullanım alışkanlığı artmıştır. Bu artışı desteklemek için, internet servis sağlayıcıları yüksek kalitede hizmet sunmak için çalışmalar yapmaktadırlar. Bu rekabet ortamında öne çıkan bir husus, aslında son derece ciddi bir konu olan güvenliktir. DDoS saldırılarında, hizmetin bozulması için çok kısa sürede, örneğin bir dakikanın biraz altında çok sayıda paket veya yüksek hacimli trafik üretildiğinde hızlı bir yanıt verilmektedir.

Güvenlik uzmanları; ağ kaynaklarına yönelik iç ve dış tehditlerin hızla ortaya çıkmasını önlemek için Saldırı Algılama Sistemi (IDS: Intrusion Detection System) ve Saldırı Önleme Sistemi (IPS: Intrusion Prevention System) gibi çeşitli yaklaşımlar sunmaktadır.

1.3.1. DDoS Algılama Sistemi

Saldırı algılama sistemi ağ trafiği ve kötü amaçlı sistem etkinlik faaliyetlerini izlemektedir. IDS izleme, algılama ve tepki modüllerinden oluşmakta olup Şekil 1.18'de sunulmuştur.



Şekil 1.18. DDoS Algılama Sistemi (Bhattacharyya ve Kalita, 2016)

1.3.1.1. İzleme

Bu modül ağda kullanılan hizmetlerin ve etkinliklerin izlenmesine olanak tanır. Bu izleme faaliyetlerini gerçekleştirmek için, ağın çeşitli noktalarından ağ durumu hakkında gerekli bilgiler toplanır. Bu modül aynı zamanda ağ içindeki yetkisiz servislerin belirlenmesine yardımcı olmaktadır. Bu yetkisiz servislerin tanımlanması için, yalnızca dış trafiğe değil, aynı zamanda iç trafikte de izlenmektedir.

1.3.1.2. Algılama

Algılama modülü ağdaki yanlış veya anormal davranışları tespit ederek güvenlik uzmanına raporlar hazırlamayı amaçlamaktadır. Algılama modülünden saldırı girişimini durdurması beklenebilir, ancak bu durum sistem tasarımı için yanıltıcı bir seçimdir. Saldırı algılama modülü öncelikle muhtemel olayları veya faaliyetleri belirleme ve bunları zamanında anlamlı bir şekilde raporlamaya odaklanması gerekmektedir. Algılama modülü yanlış kullanımları veya anormallikleri içeren olası güvenlik ihlallerini tespit etmek için ağ trafik bilgilerini incelemektedir.

1.3.1.3. Tepki

DDoS algılama sisteminin pasif ve aktif iki temel bileşeni birbiri ile etkileşimli olarak çalışmaktadır. Bir dizi prosedürden oluşan pasif bileşen; sistem yapılandırma dosyalarının incelenmesinde, uygun olmayan ayarları tespit etmede, istenmeyen parolaları saptamada, parola dosyalarının kontrol edilmesinde ve politika ihlallerini tespit etmek için diğer sistem alanlarının incelenmesine katkı sağlamaktadır. Başka bir prosedür setinden oluşan aktif bileşen aksine bilinen saldırı yöntemlerine tepki verir ve sistem tepkileri üretir. Şüpheli durumlarda; uyarı görüntüleme, log kayıtları tutma veya yöneticiyi sistemin başına çağırmak gibi tepkileri vermektedir.

1.3.2. DDoS Algılama Teknikleri

DDoS saldırılarının tespiti genel olarak iki kategoride incelenmektedir: Kötüye Kullanım Algılama (Misuse Detection) ve Anomali Tabanlı Algılama (Anomaly-based Detection.). Kötüye Kullanım Algılama Tekniği, daha önce bilinen DDoS

saldırı türlerini belirlemek için yakalanan ağ trafiğini (İmza, kural veya etkinlikleri) inceler. Bu tür algılama teknikleri, genellikle yanlış algılama sayısının düşük olduğu yüksek algılama seviyesini gösterir. Bununla birlikte, Kötüye Kullanım Algılama tekniği, bilinmeyen DDoS algılama türlerini tespit edemez. Anomali tabanlı DDoS tespit teknikleri, bilinen tiplerin saptanmasına ek olarak yeni saldırı tiplerini belirlemeyi amaçlamaktadır. Bu tür teknikler ağ trafiğini analiz eder ve erken aşamada alışılmadık kalıpları saptamaya çalışır.

1.3.2.1. Kötüye Kullanım DDoS Algılama Tekniği

Kötüye kullanım tespitinde kötü olduğunu bilmediğimiz her şey normaldir. Saldırı imzalarını IDS'lerde kullanma, bu yaklaşımın bir örneğidir. IDS'nin algılama doğruluğu açısından performansı, bilinen saldırı bilgisinin ne kadar yeterli olduğu ve algılama motorunun algılama sırasında ne kadar iyi kullanabileceğine bağlıdır. Bilinen saldırılar hakkında iyi hazırlanmış veriler, bu algılama yaklaşımını etkin bir şekilde kullanılmasına ve yüksek doğrulukla algılama yapmasını sağlar. Bu teknik imza tabanlı ve kural tabanlı DDoS algılama tekniği olarak ikiye ayrılır.

1.3.2.1.1. İmza Tabanlı DDoS Algılama Tekniği

İmza tabanlı algılama tekniğinde, saldırı kalıp dizileri ve imzaları depolanır. Saldırı Algılama Sistemi veri tabanında önceden depolanmış ön tanımlı saldırı imza kümeleri ile eşleştirerek saldırıları belirlemeye çalışır. Başarılı olduğunda sistem alarm verir. Bu yaklaşımda, saldırının anlamsal özellikleri analiz edilir ve saldırı imzaları oluşturmak için ayrıntılar kullanılır. Veri tabanını oluşturulmasında bilinen saldırıların imzaları kullanır.

1.3.2.1.2. Kural Tabanlı DDoS Algılama Tekniği

Kural Tabanlı Algılama sistemlerinde koşul sorgulaması yaparak kurallar oluşturmaktadır. Güvenlik uzmanları, saldırıları analiz ederek kurallar geliştirir ve bunları daha sonra, kötüye kullanım tespiti için izlenen veriler (log) ile karşılaştırmak için IDS'nin çıkarsama modülleri tarafından kullanılan koşullu kurallara dönüştürürler. Bu şekilde algılama yaklaşımı kullanmaktadır.

1.3.2.2. Anomali Tabanlı DDoS Algılama Tekniği

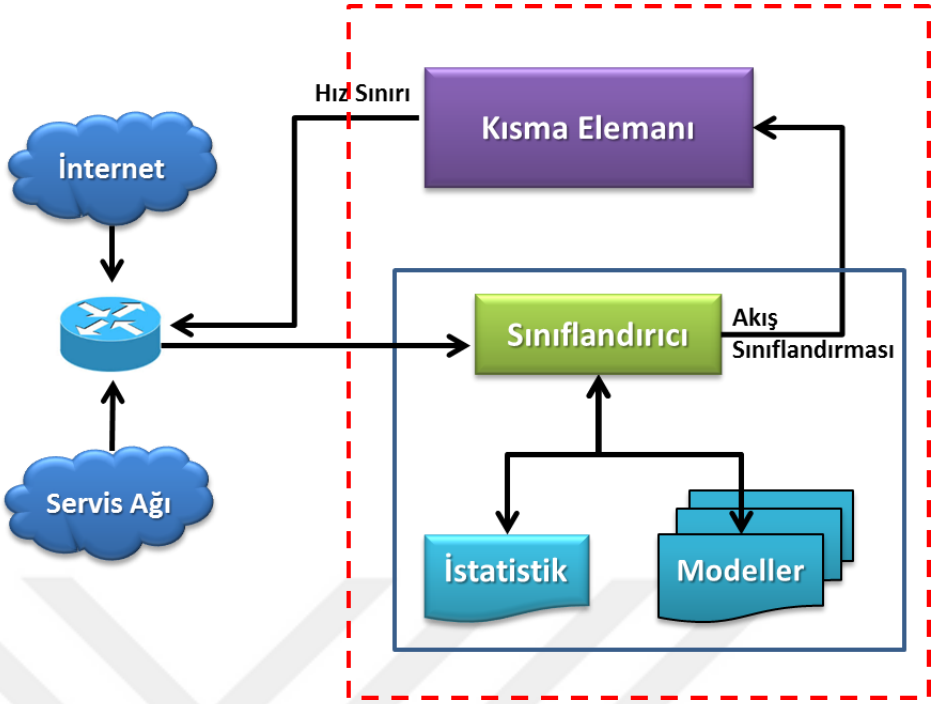
Anomali Tabanlı DDoS Algılama tekniğinde önce kullanıcı veya sistemin olabileceği normal davranışlar belirlenir. Bir işlem normal davranış veya kalıptan belirgin bir şekilde saparsa, anomali olarak kabul edilir. Böylece, güvenlik uzmanı sistem için normal bir kural dizini kurabilirse, normal profilden farklı olan tüm sistem durumlarını da işaretlenebilir.

Anomali Tabanlı DDoS Algılama sisteminin en önemli avantajı bilinmeyen saldırıları tespit edebilmesidir. Anomali tabanlı DDoS algılama yaklaşımlarına dayalı (Thottan ve ark., 2010) yazılım tabanlı DDoS savunma çözümleri ve donanım tabanlı ağ güvenliği çözümleri geliştirilmiştir. Ayrıca yüksek yoğunluklu DDoS saldırılarına karşı, istatistiksel, makine öğrenme, veri madenciliği ve bilgi tabanlı çeşitli yaklaşımlar da geliştirilmiştir.

1.3.2.2.1. İstatistiksel DDoS Algılama Tekniği

İstatistiksel yöntemlerin etkinliği, anomali temelli saldırı tespitinde halihazırda kullanılmaktadır. İstatistiksel yaklaşım başlangıçta normal kullanıcı davranışını, sistem kullanım politikası olarak kabul ederek tanımlamaktadır. İzlenen davranış önceden tanımlanmış normal davranış eşiklerinden belirgin olarak sapması durumunda, anormal bir aktivite veya saldırı olarak değerlendirilir. Sapma, kümülatif toplam, korelasyon, entropi, karşılıklı bilgi katsayısı ve kovaryans gibi çeşitli istatistiksel ve bilgi teorik ölçümleri kullanılarak ağ anomalileri saptanmaktadır. İstatistiksel DDoS algılama tekniğinde farklı birçok yaklaşım bulunmaktadır.

D-WARD (Mirkovic ve Reiher, 2005b), saldırıları algılamak ve durdurmak için Saldırı Kaynağı-Hedef arasındaki ağlarda konuşlandırılan istatistiksel gözlem yaklaşımı ile oluşturulan DDoS savunma mimarisi tasarlamıştır. Giden trafik ve adres seti ile şebekenin geri kalan kısmı arasındaki iki yönlü trafiği izlemek amacıyla, önceden belirlenmiş bir adres seti yapılandırılmaktadır. D-WARD'a ait DDoS Savunma Mimarisi Şekil 1.19'de gösterildiği gibi Sınıflandırıcı ve Kısma Elemanı mimarinin temel bileşenleridir. D-WARD'da trafik bilgileri çevrimiçi olarak toplanmakta ve bu bilgiler önceden tanımlanmış normal trafik modelleriyle karşılaştırıldıktan sonra uygun olmayan trafik hız sınırlamasına tabi tutulmaktadır. Hız sınırlaması dinamik olarak ve akış davranışı değiştiği ile ayarlanmaktadır. Bu nedenle, yanlış sınıflandırılmış normal trafik hızlı bir şekilde tekrardan iyileştirilmektedir. Bununla birlikte ölçeklenebilirlik ve yeni saldırıların gerçek zamanlı algılanması DDoS algılama sistemi için önemli bir husustur.



Şekil 1.19. D-WARD DDoS savunma mimarisi (Mirkovic ve Reiher, 2005b).

Chen ve Ark. (2009) iki örneklemeli T-testine dayanan etkili bir DDoS algılama tekniğini sunmaktadır. Bu yaklaşım ilk olarak normal trafiğe ait SYN Varış Oranı (SAR: SYN Arrival Rate) örneklem dağılımlarını araştırılır. Normal bir dağılıma uyup uymadığı kontrol edilir. DDoS saldırı trafiği ile meşru trafik arasındaki SAR sapması hesaplanmakta ve SYN ve ACK paketlerinin sayıları arasındaki fark bulunmaktadır. Önemli bir farklılık bulunursa, trafiğin saldırı trafiği olabileceği onaylanır. Bununla birlikte, düşük oranlı bir DDoS saldırısı olması durumunda, varış hızı testi yararlı olmayabilir ve bu nedenle, saldırı amacına ulaşabilir (Chen ve Ark., 2009).

Jin ve ark. tarafından geliştirilen Çok Değişkenli Korelasyon Analizi (MCA: Multivariate Correlation Analysis) ağ trafiğinde ani değişimleri ölçmek için etkili bir yaklaşımdır. SYN Flooding saldırı algılama modelinde (Jin ve Yeung, 2004) MCA sayesinde bir ağdaki anormal trafiği basit ama etkili bir şekilde tanımlamak için kullanılabileceğini göstermektedir.

1.3.2.2.2. Makine Öğrenme ve Veri Madenciliği DDoS Algılama Teknikleri

Makine öğrenme (ML: Machine learning) ve veri madenciliği tekniğinde; sistem programlanmadan ortamdan öğrenme özelliğine sahiptir. Bu ise kaynakları ağ saldırılarına karşı etkili algılama mekanizmalarının geliştirilmesinde önemli bir rol oynamaktadır (Bhattacharyya ve Kalita, 2016).

Hwang ve ark. (2003) sunucu, yönlendirici ve ana bilgisayar gibi ağ kaynaklarını DDoS saldırılarına karşı korumak için NetShield olarak adlandırılan verimli bir DDoS savunma çözümü sunmaktadır. NetShield IP üzerinden veri madenciliğini kullanarak DDoS saldırılarını tespit edecek şekilde tasarlanmıştır. Bu algılama yazılımı yalnızca DDoS saldırılarına karşı savunmakla kalmaz, aynı zamanda diğer zararlı ağ solucanları ve virüsleri de tespit edebilmektedir. Bu sayede saldırıların önlenmesi ve saldırı raporunun hazırlanmasını sağlamaktadır (Hwang ve ark., 2003).

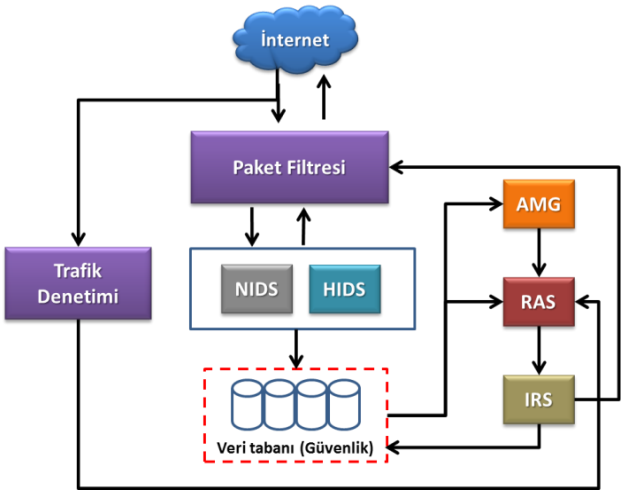
NetShield yazılımı, USC Kablosuz İnternet Güvenlik Laboratuvarı'nda simülatör kullanılarak tasarlanmıştır. Paket filtreleme, trafik denetleme ve güvenlik veri tabanı sahip NetShield sistemi; ayrıca aşağıdaki temel modülleri kullanmaktadır;

a) Bilgisayar tabanlı saldırı algılama sistemi (HIDS: Host-based Intrusion Detection System) ile ağ tabanlı saldırı algılama sisteminden (NIDS: Network-based Intrusion Detection System) oluşan bir algılama modülü,

b) Alarm matris üreteci (AMG: Alarm Matrix Generator),

c) Risk değerlendirme sistemi (RAS: Risk Assessment System),

d) Yetkisiz Giriş Tespit Sistemi (IRS: Intrusion Response System) modüllerinden oluşmaktadır. Modül yapısı Şekil 1.20'de sunulmuştur.



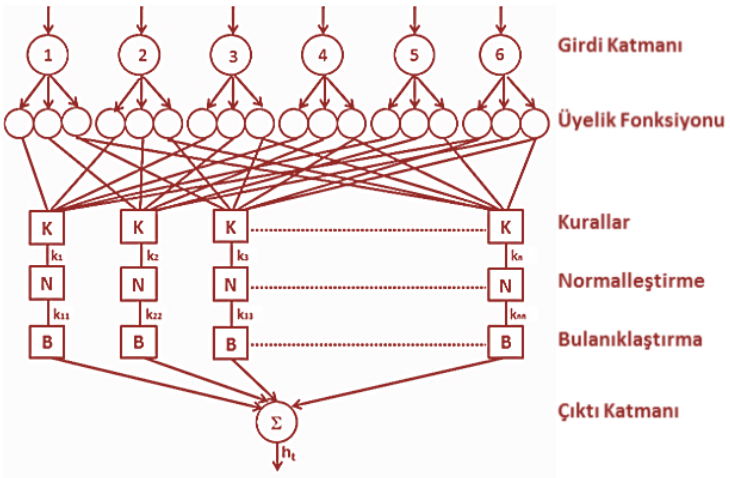
Şekil 1.20. NetShield yazılım yapısı (Hwang ve ark., 2003)

Tüm saldırı bilgileri merkezi olarak korunan ve dinamik olarak güncellenen bir güvenlik veri tabanında saklanmaktadır. HIDS, ağdaki C&C sunucuları veya köle bilgisayar faaliyetlerini tanımlamak üzere tasarlanmıştır. NIDS, gelen trafiği analiz ederek DDoS saldırılarını aktif olarak tespit etmektedir. Trafik denetimi modülü, trafik özelliklerini tanımlamak ve düzensiz trafiğin tespit etmek maksadıyla ağ trafiğini izlemektedir. Bir saldırı tipi teyit edildiğinde, AMG modülü alarm üretmekten sorumludur. NetShield DDoS saldırılarının bazı risklerini azaltabilmekte ancak bazılarını kısmen engellenebilmektedir.

1.3.2.2.3. Basit Hesaplama DDoS Algılama Tekniği

Basit hesaplama tekniğinde; bulanık mantık, sinirsel hesaplama, evrimsel hesaplama, makine öğrenimi ve olasılıklı mantık ana yaklaşımları kullanılmaktadır. Bu yöntem özellikle problem hakkındaki bilgilerin yetersiz olduğu durumlarda, problemlerin çözümünde faydalı olmaktadır. Ayrıca düşük hata paylı alarm sistemi sayesinde, anormal trafiği algılama doğruluğunun yüksek olması ve ağ güvenliğinin sağlanmasında meşru trafiği ayırabildiği araştırmacılar tarafından doğrulanmıştır.

DDoS algılama sistemi algılama hassasiyetinin yüksek olması maliyeti yukarı doğru çekmektedir. Bazı araştırmacılar, işlem maliyetini en aza indirgemek için uyarlanabilir ve aşamalı sınıflandırmayı tercih etmektedirler. Belirsiz veya kesin olmayan bilgilerin varlığı, DDoS saldırı tespit yöntemlerinin performansını analiz ederken ve değerlendirirken önemli bir konu olarak ortaya çıkmaktadır. Her iki zorluğun üstesinden gelmek için uyarlanabilir, aşamalı ve yumuşak hesaplama yaklaşımları kullanılmaktadır. Kumar ve ark. (2013) basit hesaplama tekniklerinden Uyarlanabilir Hibrit Nöro-Bulanık Çıkarım Sistemi (ANFIS: Adaptive And Hybrid Neuro-Fuzzy Inference Systems) kullanarak NFBoost olarak adlandırılan bir DDoS algılama sistemi geliştirmişlerdir. Tek bir katman veya sınıflandırıcı önyargılı olabilir ve trafik örneklerinin eğitiminde hata yapabilir. Bu nedenle sınıflandırıcıların birkaç katmandan geçecek şekilde oluşturulması ve çıktılarını uygun bir kombinasyon işleviyle birleştirerek bu önyargıları giderilebilir. Şekil 1.21'de Uyarlanabilir Hibrit Nöro-Bulanık Çıkarım Sistemi yapısı gösterilmektedir. NFBoost'un DDoS saldırılarını% 99.2 doğrulukla ve düşük hata payı ile alarmlar oluşturabildiği tespit edilmiştir (Kumar ve ark., 2013).



Şekil 1.21. Uyarlanabilir hibrit nöro-bulanık çıkarım sistem yapısı (Kumar ve ark., 2013)

Bir başka çalışmada, Jalili ve ark. (2005) istatistiksel ön-işlemci kullanarak, denetimsiz sinir ağı uygulayan etkili bir DDoS algılama sistemi geliştirmişlerdir.

Eğitim vektörünün oluşturulmasında ön-işlemci kullanılarak ağ trafiğine ait istatistiksel bilgiler elde edilmektedir;

- ICMP paketlerinin yüzdesi,
- UDP paketlerinin yüzdesi,
- TCP paketlerinin yüzdesi,
- TCP paketlerindeki SYN yüzdesi,
- TCP paketlerinde SYN + ACK yüzdesi,
- TCP paketlerinde ACK yüzdesi,
- Ortalama paket üstbilgi boyutu,
- Ortalama paket veri boyutu gibi istatiksel bilgiler, DDoS saldırılarını tanımlanmasında kullanmaktadır. Paket trafiğini daha küçük zaman aralıklarında değerlendirmek için τ saniye uzunluğuna bölünür. Her bir zaman aralığı için yukarıda sayılan özellikler elde edildikten sonra, meşru veya DDoS saldırısı olarak tanımlamak için sinir ağı kullanarak ağ trafiğini analiz etmeyi destekleyen bir eğitim vektörü oluşturulur. Yöntemlerinin değerlendirilmesi sırasında, τ'nun boyutu veya uzunluğu, sinir ağı ile ilişkili parametreler gibi birkaç önemli parametrenin etkileri üzerine yapılan çalışmada saldırı trafiğini % 94.9 oranla tespit edelebildiği görülmektedir.

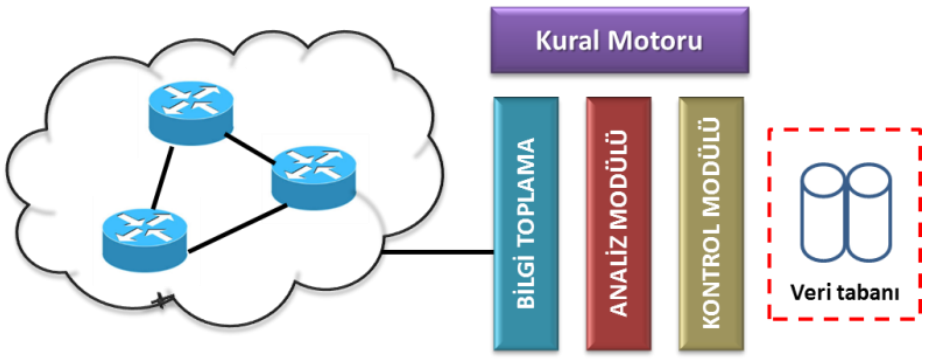
1.3.2.2.4. Bilgi Tabanlı DDoS Algılama Tekniği

Bilgi tabanlı DDoS saldırı algılama yaklaşımında, bir güvenlik çözümü geliştirirken daha önceki DDoS saldırı geçmişinden elde edilen veriler ön bilgi olarak kullanılmaktadır. Geçmiş bilgilere dayandırılarak alınan güvenlik tedbirleri; bilinen saldırı türleri için oluşturulan bir dizi kural veya imzanın algılama sırasında gelişen ağ olayları ile eşleştirilmesiyle yapılmaktadır. Bir eşleşme varsa alarm sistemi devreye girmektedir. DDoS saldırılarına karşı çeşitli bilgi tabanlı savunma teknikleri geliştirilmiştir. Bu teknikler çoğunlukla dört farklı kategoride; kural tabanlı

filtreleme, imza analizi, haritaları self organize etme ve durum geçiş analizini kapsamaktadır.

Kural tabanlı filtreleme bilinen DDoS saldırılarını azaltmanın etkili bir yoludur. İstatistiksel yöntemlerden farklı olarak, kural tabanlı filtrelemede genellikle kurulum ve algılamayı başlatmak için daha az zamana ihtiyaç vardır (Holl, 2015). Etkili bir kural tabanlı filtre, bilinen DDoS saldırı türleri için algılama performansını %100'e kadar çıkarmaktadır. Dikkatli bir şekilde oluşturulmuş kural tabanlı bir filtre sayesinde hata payı çok düşük seviyelere çekilebilir. Bununla birlikte, bilinmeyen güvenlik açıkları ve yeni tür DDoS saldırıları karşı ilgili kurallar mevcut olmadığından kural tabanlı filtreler etkisizdir. DDoS saldırılarında büyük değişiklikler olması durumunda, kural veri tabanı büyümekte ve güvenlik tedbirleri için gerekli sürede uzamaktadır. Son zamanlarda yapılan DDoS saldırı senaryolarını göz önüne alındığında saldırıların büyük ölçekli ve geçmiş saldırılardan farklı olduğu gözlemlenmektedir.

Kim ve ark. (2008) birden fazla DDoS saldırı tipinin hızlı bir şekilde algılanmasını sağlamak için kural tabanlı savunma yöntemi sunmaktadırlar. Yöntemlerinin genel çerçevesi Şekil 1.22'de gösterilmektedir.

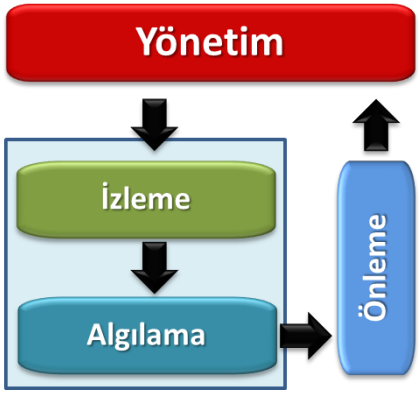


Şekil 1.22. Kural tabanlı DDoS savunma yöntemi (Kim ve ark., 2008)

Yöntemde, önce belirli bir zaman aralığı için trafik verileri toplanmakta sonrasında da bu veriler analiz edilmektedir. Yöntem, anormal trafiği tanımlamak için bir grup kurala sahiptir. DDoS saldırı türlerini gerçek zamanlı olarak algılamak için bu kural grubunun etkili bir şekilde kullanılması amaçlanmaktadır. Analiz sırasında TCP ve UDP ait bilgi paketleri ve varış noktasına ait bilgiler kullanılmaktadır. Analiz sonucu kritik değerler aşmıyorsa, işlem meşru trafik olarak değerlendirilmektedir. Aksi halde, anormal olduğu ve buna karşılık gelen kaynak IP'lerin bloke edilmesinin gerektiği değerlendirilir.

1.4. DDoS Saldırı Önleme Sistemi

Saldırı Önleme Sistemi (IPS: Intrusion Prevention System) Saldırı Algılama Sisteminin (IDS) "geliştirilmiş" sürümü olarak düşünülmüştür (Desai, 2009). Her ikisi sistemde ağ trafiği ve kötü amaçlı sistem etkinlik faaliyetlerini izlemektedir. Bununla birlikte, saldırı önleme sisteminin IDS'den farklı olarak, tespit edilen saldırıları aktif bir şekilde engelleyebilmesidir. IPS genel olarak; sistem alarmları üretmesi ve kötü amaçlı paketlere ait IP adreslerinden gelen trafiğin engellemesini amaçlamaktadır. Saldırı önleme sistemi genel görünümü Şekil 1.23'de gösterilmektedir. İzleme ve algılama bileşeni ile IDS'deki yapıya benzesede IDS'deki reaksiyon/tepki bileşeni yerine önleme prosedürleri bulunmaktadır. Önleme teknolojisinde şüpheli trafiğin davranış modeline dayanan bir dizi prosedürler yönetim sistemi ile etkileşimli olarak çalışmaktadır. Yönetimin sorumluluğu trafik akışını yönetmek ve önleme teknolojisi tarafından sağlanan prosedürleri uygulamaktır.



Şekil 1.23 DDoS saldırı önleme sistemi genel görünümü (Bhattacharyya ve Kalita, 2016)

1.4.1 DDoS Önleme Teknikleri

DDoS saldırı önleme sistemi, tespit edilen tehditleri gerçek zamanlı olarak engellenmesi ve hedef sisteme yakın hareket etmesini önleyen bir yazılım veya donanım aygıtı tarafından gerçekleştirilmesidir. Günümüz internet altyapısının güvensizliği ve internet servis sağlayıcılarının kendi altyapı hizmetlerindeki DDoS saldırılarına karşı tek başlarına yeterli olamaması sistem açıcından önemli bir ihtiyacı ortaya çıkarmaktadır.

DDoS saldırılarının gerçek zamanlı olarak önlenmesi ağ güvenliği için ciddi bir problemdir. IPS'yi IDS'nin bir uzantısı olarak düşünülebilir. IPS ve IDS'ler arasında; saldırıları ve ağ trafiğini inceleme sürecindeki kritik farklılıklar bulunmaktadır. İki sistem hem kötü amaçlı veya istenmeyen trafiği tespit etmekte, ancak alarm üretimlerinde farklılıkları bulunmaktadır. Etkili bir önleme sistemi için önceden algılayabilme kabiliyetine sahip olması ve sonrasında saldırı kaynaklarını belirleyebilecek uygun eylemleri başlatabilmesi gerekmektedir. DDoS koordine edilmiş bir saldırı olduğundan saldırı kaynaklarının gerçek zamanlı olarak tanımlanması kolay değildir. Ayrıca, saldırı paketlerindeki kaynak IP adreslerinin sahte olması, DDoS önleme girişimlerinin işini zorlaştırmaktadır.

Etkin bir DDoS önleme sisteminin geliştirilmesi için gerçek saldırı kaynaklarının belirlenmesi çok önemli bir husustur. Gerçek saldırı kaynaklarının tanımlanmasında; internetin güvensiz ve merkezi olmayan yapısı nedeniyle son derece zor bir görev olmakla birlikte, yakın geçmişte bu konuda birçok yeni yaklaşım geliştirilmiştir. IP Geri İzleme (IP traceback) ve Filtreleme DDoS saldırılarındaki gerçek kaynakların tanımlanmasında kullanılan önemli birer yöntemlerdendir.

1.4.1.1 IP Geri İzleme Tekniği

DDoS saldırısında saldırganlar sahte IP adreslerini kullanarak hedef bilgisayara saldırı paketleri göndermekte ve bu maksatla köle bilgisayarlar kullanılmaktadır. IP geri izleme işlemi manuel veya otomatik olarak yapılabilmektedir. Router üzerinden yapılacak geri izleme işlemi sayesinde saldırı kaynak IP adreslerinin tespiti yapılabilmektedir. Genellikle bir Router'dan diğer bir Router'a hop-by-hop traceback yöntemi ile geri izleme yapılmaktadır. Bu nedenle, saldırı kaynağının başarılı bir şekilde tanımlanması için ağlar arasındaki ilişkinin incelenmesi son derece önemlidir. Manuel olarak yapılan geri izleme süreci sıkıcı ve zaman alıcı bir işlemdir. Süreci hızlandırmak için otomatik izleme sistemi geliştirmiştir. Etkili bir geri izleme mekanizması aşağıdaki özelliklere sahip olması gerekmektedir:

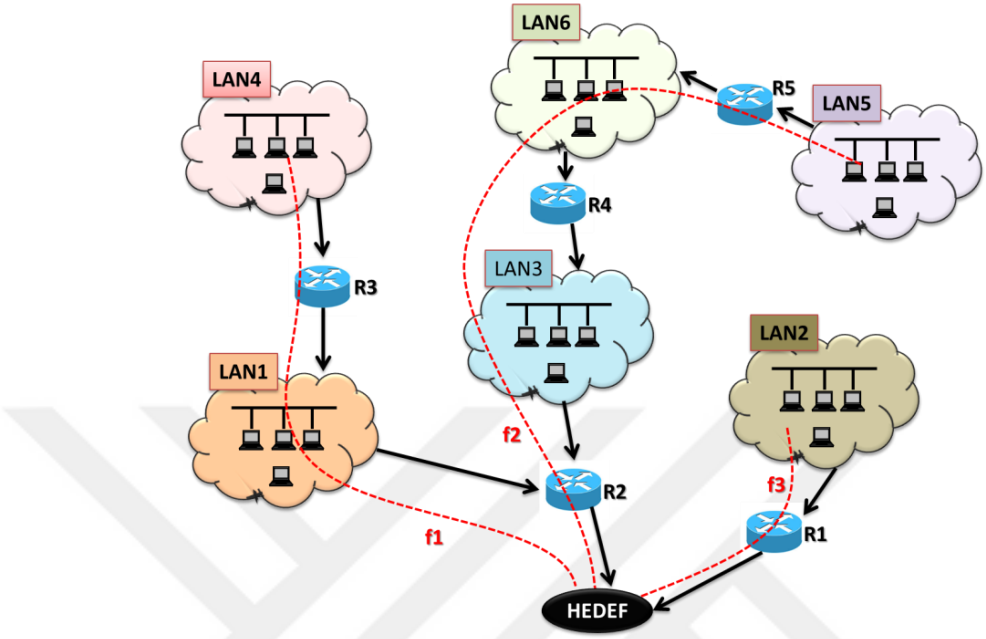
- Geri izleme mekanizması maliyet-etkin olmalı,
- İnternet servis sağlayıcıların katılımı düşük olmalı,
- Router ve switch için ilave bellek maliyeti oluşturmamalı,
- Düşük ağ yükü üretmeli,
- Geri izleme sisteminin geliştirilmesi sorun teşkil etmemeli,
- Geri izleme mekanizması, orijinal saldırı kaynağını tek bir paket yardımı ile tespit edebilmelidir.

Yu ve ark. (2011) tarafından bir örneği geliştirilen geri izleme örnek ağı Şekil 1.24'de sunulmuştur. Bu örnek ağda, 6 adet ağ (LAN1, LAN2, • • •, LAN6) ve beş adet Router (R1, R2, • • •, R5) kullanılmıştır. LAN1, LAN3 ve LAN6'dan çoklu saldırı ile tek bir bilgisayar hedef alınmıştır. Şekilde n ormal ağ akışı ve saldırı akışlar ayrı olarak gösterilmektedir. Şekil 1.24'de, f3 normal ağ akışını, f1 ve f2 ise saldırı ve normal akışını birlikte göstermektedir. Tipik bir DDoS saldırısında ağ yoğunluğu kısa bir zaman aralığında önemli ölçüde artmaktadır. Böylece, R2 ve R4 Router'larında önemli bir değişiklik gözlemlenebilir. Buna karşılık, R1, R3 ve R5'de bu tür değişiklikler veya saldırılar bulunmamaktadır. Bu tür değişiklikler hedef tarafından algılanırsa, genellikle saldırıya karıştığından şüphelenilen LAN'lar geri dönmeye çalışır. Yönelticiler trafikteki değişimleri ölçmek için bilgi metriklerini (entropi) kullanılabilir. Başka bir deyişle, belirli bir zaman aralığı için Router'daki akış değişiklikleri ölçebilir. Hedef makinedeki önemli akış değişimlerinin entropi açısından keşfedilmesi, burada yüksek bir oranlı saldırı kaynaklarının R2'nin arkasında olduğunu, ancak R1'in arkasında olmadığını tahmin edilmesi anlamına gelmektedir. Çünkü R1'de önemli bir entropi varyasyonu algılanmamıştır (Yu ve ark., 2011).

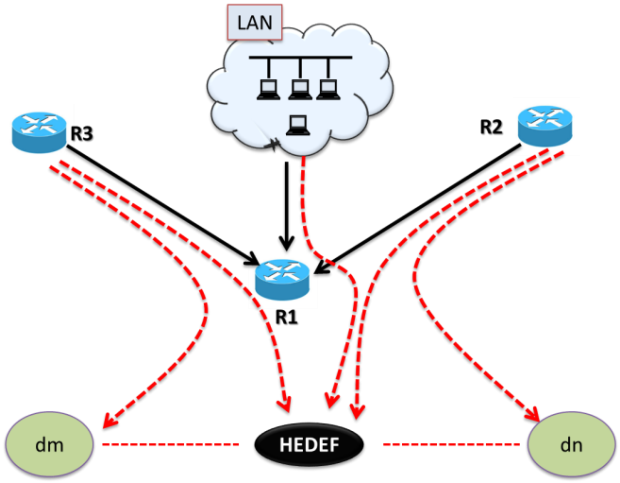
Böylelikle yönetici DDoS saldırılarının olası kaynağını bulmak için R2'ye bir geri izleme isteği gönderecektir. Algılanan entropi varyasyon ile, R2 DDoS saldırılarının iki kaynaktan yani LAN1 ve LAN3 arkasında olduğunu belirleyecektir. Ardından, geri izleme isteği LAN4 ve LAN6, diğer bir deyişle R3 ve R4'ün kenar Router'larına iletilecektir. Benzer şekilde, her iki yönlendiricide de entropi varyasyonları hesaplanacak ve herhangi birinde veya her iki Router'da önemli bir değişiklik tespit edilirse, buna göre hareket edilecektir.

R3, saldırı kaynaklarının LAN1'den geldiğini çıkarabilir. Bununla birlikte, R4, saldırganların LAN3'ten olduğunu ve R4'ün arkasında olduğunu göstermektedir.

Buna göre, geri izleme isteğinin LAN6'dan gelen saldırıyı bulmak için daha ileri yönelticiler, örneğin R5'e iletilmesi gerekir. Ağ yönetici saldırı akışını izlemesi için gereken yöntem Şekil 1.25'dedir.



Şekil 1.24. Geri izleme yöntemi örnek ağı (Yu ve ark., 2011)



Şekil 1.25. Saldırı akışının izlenmesi (Yu ve ark., 2011)

Böyle bir entropiye dayalı geri izleme düzeni yalnızca aşağıdaki varsayımlar geçerli olduğunda yararlı ve etkili olacaktır.

Varsayım 1: DDoS saldırısı sırasında ağ trafiğinde değişim çok kısa bir sürede, örneğin saniyeler içinde gerçekleşir. DDoS saldırısı olmadığı durumlarda, bu tür değişiklikler meydana gelebilir ancak daha uzun bir süre yani dakikalarca sürmektedir.

Varsayım 2: Yüksek oranlı bir DDoS saldırısı sırasında, saldırı paketleri binlerce köle bilgisayar (Yu ve ark., 2011) tarafından üretilir ve dolayısıyla saldırı paketlerinin sayısı normal veya meşru ağ akışı ile karşılaştırıldığında önemli derecede yüksektir.

Varsayım 3: Hem saldırı hem de saldırı olmayan durumlarda, belirli bir Router'daki ağ akış sayısı sabittir.

Varsayım 4: Belli bir zaman aralığında, yalnızca bir DDoS saldırısı gerçekleştirlmesi varsayılmaktadır.

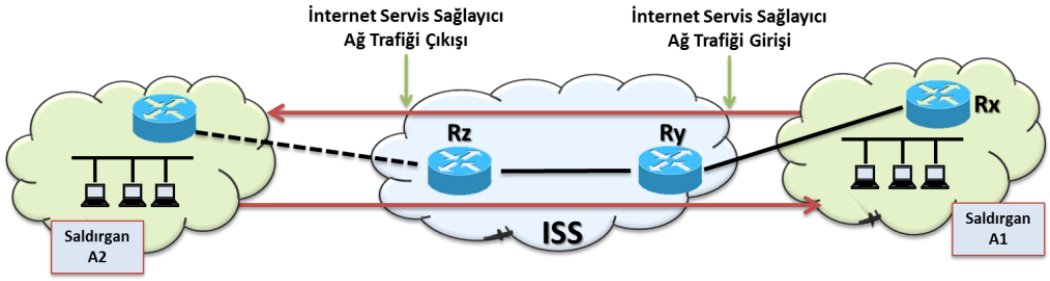
1.4.1.2 Filtreleme Teknikleri

Filtreler, ağ kaynaklarını DDoS saldırılarına karşı korumak için güçlü bir mekanizmadır. Ağ güvenliği araştırmacıları tarafından birkaç farklı filtreleme tekniği geliştirilmiştir. Sahte IP adresleriyle gerçekleştirilen DDoS saldırı trafiğini karşı geliştirilen üç farklı filtreleme tekniği anlatılacaktır.

1.4.1.2.1 Giriş ve Çıkış Filtreleme Tekniği

Giriş ve çıkış filtreleri, DDoS saldırılarının önlenmesinde çok faydalıdır. Giriş filtrelemede ağa gelen trafiği filtrelemek için kullanılırken çıkış filtreleme de ağdan

çıkan trafiği filtrelemek üzere uyarlanır (Tao ve ark., 2007). Giriş ve çıkış filtreleme kurallarını belirlerken, karışıklığa ve çatışmaya engel olmak için referans noktası belirlenir. Bu iki filtreleme tekniğine örnek olarak, Ferguson ve Senie (2000) orijinal filtreleme önerisi Şekil 1.26'da gösterilmektedir.



Şekil 1.26. Giriş ve çıkış filtreleme yöntemi örnek ağı (Ferguson ve Senie, 2000)

Yukarıdaki şekilde A firması internet servis sağlayıcısı tarafından bir kurum ya da kuruluşa verilen internet erişim şeması sunulmaktadır. Rx Router'ı ISS A firmasının Ry Router'na bağlıdır. ISS A, Rz Route'ı ile farklı ağlara bağlıdır. Öneriye göre, giriş ve çıkış filtreleri önceden belirlenmiş kaynak IP adres aralığıyla eşleşiyorsa giriş-çıkış yapan paketlere izin vermektedir.

Bir senaryo dahilinde, Saldırgan A1'in kurumun ağının içinden sahte IP adreslerine ait paketleri sunucuya gönderdiğini varsayılmaktadır. Ayrıca ISS A'nın yönlendirici Ry'nin bir giriş filtresi ile donatıldığını ve kurum ağına bağlı olduğu varsayılmaktadır. Giriş filtresinin yalnızca 202.141.129.0/24 kaynak IP adresleri olan paketlere izin vereceğine ilişkin bir kural varsayılmaktadır. Saldırgan A1'e ait sahte IP adresinin paketlerinde böyle bir önek bulunmuyorsa, filtre bu paketleri Ry'ye geçişini engellemektedir. Ry tarafından sağlanan böyle bir filtreleme yapısına giriş filtresi denmektedir.

Benzer şekilde, başka bir senaryoda, A2 saldırganının hem ISP A'nın hem kurum ağının dışında olduğu ve sahte IP adresleri bulunan paketleri kurumun

ağındaki sunucuya gönderdiği varsayılmaktadır. Ayrıca kaynak IP adreslerinin 202.141.129.0/24 dışındakilerinin izleneceği şeklindedir. Önceki örnekte olduğu gibi giriş filtresi ile donatılmış olan Rz, önceden tanımlanmış IP adres aralığıyla eşleşmediğinden bu paketleri engelleyecekdir. Rz'de gerçekleştirilen böyle bir filtreleme işlemi giriş filtresi, filtreleme işlemi Ry'de gerçekleştirilirse çıkış filtrelemesi olarak adlandırılır.

1.4.1.2.2 Yönlendirici Tabanlı Paket Filtreleme

Yönlendirici tabanlı paket filtreleme, Park ve Lee (2001)'nin geliştirdiği giriş filtrelemesinin bir uzantısıdır. IP paketinde herhangi bir sapma saptanırsa kaynak adresin sahte olduğu ve buna göre paket filtrelenme uygulanır. Tekniğin çalışma prensibinde internet bir dizi yönlendirme alanına (AS: Autonomous Segments) bölünmektedir. Her bir AS, kurum ve kuruşlara ait birden fazla ağı temsil etmektedir. Kenar Router'ları Geçiş Protokolü (BGP: Border Gateway Protocol) olarak adlandırılan protokolleri kullanarak AS'ler arasındaki trafik yönlendirmekten sorumludur. Ayrıca bu Router'lar kullanılan topolojiye bağlı olarak birden fazlar kenar Router'ları ile çalışabilmektedir. Özetle bu teknik sahte IP adresleri içeren trafiği, BGP topolojisi hakkında mevcut bilgileri kullanarak filtrelemeye çalışmaktadır.

Yönlendirici tabanlı paket filtreleme DDoS saldırısının önlenmesi açısından birkaç avantajı olmasına rağmen, bazı dezavantajları da vardır. Son zamanlarda gerçekleşen DDoS saldırıları çok zekice planlanmaktadır. Saldırgan sahte IP adreslerini çok dikkatli seçmekte ve normal IP adresleri ve sahte IP adresleri ile birlikte kullanmaktadır. Böyle bir durumda bu filtreleme tekniğini DDoS saldırılarına karşı etkili olamamaktadır. Bu nedenle yönlendirici tabanlı filtreleme yaklaşımları özellikle dinamik internet yönlendirmesi kullanıldığında saldırı trafiğini

engelleyemez. Bu sorunu çözmek için kaynak adresi doğrulama uygulama protokolü geliştirilmiştir.

1.4.1.2.3 Kaynak Adresi Doğrulama Uygulama Protokolü

Li ve ark. (2002) kaynak IP adres bilgilerini her bağlantıda dinamik olarak güncellemek için Kaynak Adresi Doğrulama Uygulama (SAVE: Source Address Validity Enforcement) protokolünü geliştirmiştir. Önceki tekniklerde olduğu gibi, belirli bir bağlantı için kaynak IP adresleri listesinde yer almayan IP adresleri bloke edilmektedir. SAVE her bir Router bağlantıları için güncel bir tablo oluşturmakta ve IP adresleri hakkındaki bilgileri sık sık güncellemektedir. SAVE'de yönlendiricinin her bir bağlantısı için normal IP adres alanlarını önceden bilinmekte ve kararlı olduğu varsayılmaktadır. SAVE protokolünün giriş filtreleme ve RPF'ye kıyasla önemli bir avantajı, gelen link tablosu düzenli olarak güncellenmesidir. Bununla birlikte, önceki iki filtreleme tekniğindeki gibi DDoS saldırısının sadece sahte IP adreslerinden yapılmaması durumunda SAVE'de güvenli bir yöntem olmaktan çıkmaktadır.

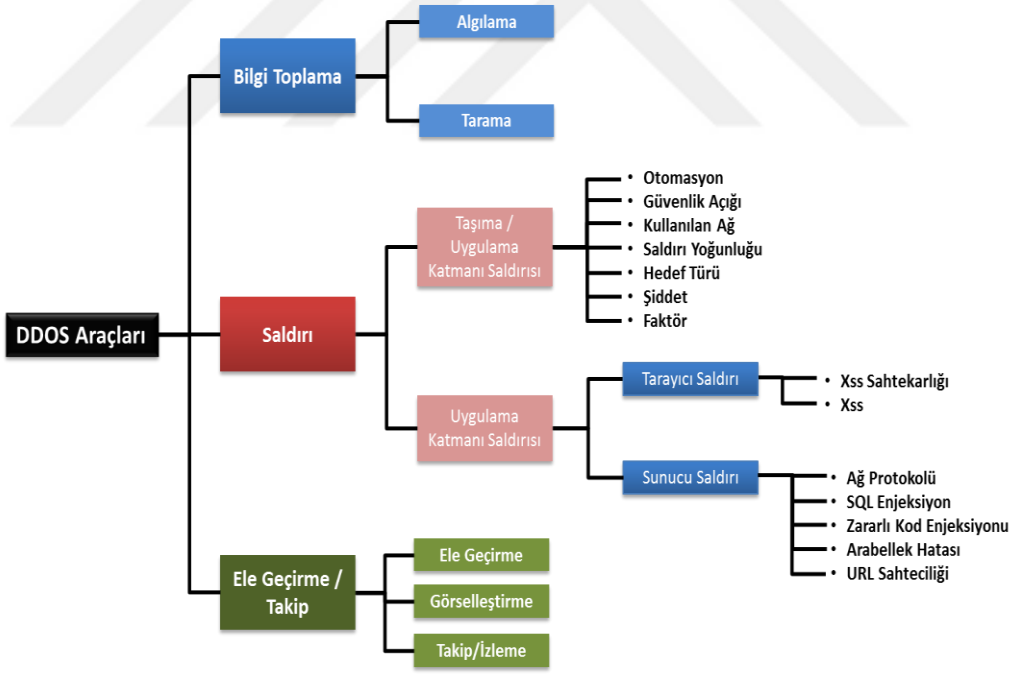
1.4.1.3 Yoğunluk Kontrolü

Yoğunluk kontrolü, önceden belirlenmiş önleme kriterlerine uyan DDoS saldırılarını önlemede etkili diğer bir yaklaşımdır. DDoS saldırı ölçütleriyle eşleşen paketlerin varış oranını kontrol etmektedir. Normal trafiğin asgari seviyede etkilenmesini engellemek için tasarlanmıştır.

1.5. DDoS Saldırılarında Kullanılan Araçlar (TOOLS)

DDoS saldırıların gerçekleştirilmesi maksadıyla saldırganlar tarafından birçok saldırı aracı geliştirilmiştir. Günümüzde internet ortamından kolayca indirebilen bu araçlara LOIC (Pras ve ark., 2010) ve HOIC gibi gelişmiş uygulamalar örnek verilebilir.

Saldırganlar genel olarak web siteleri, veri tabanları veya kurumsal ağların zayıf yönleri hakkında bilgi toplamayı hedeflemektedirler. Başlatılmak istenen saldırı sınıfı için uygun araçlar seçilerek, hedef sistemin keşfedilen zayıf noktaları istismar edilmektedir. Kullanım amacı ve özelliğine göre sınıflandırılan saldırı araçları Şekil 1.27'de gösterilmektedir.



Şekil 1.27. Saldırı araç türleri (Bhattacharyya ve Kalita, 2016)

Bu bölümde, saldırı amacıyla geliştirilen araçların özellikleri, yeteneklerini ve nasıl kullanıldıkları hakkında bilgiler verilmektedir. Bu maksatla sunulan araçlar;

- Bilgi toplama araçları,
- Saldırı başlatma araçları
- Saldırı yakalama, görselleştirme ve izleme olacak şekilde üç ana kategoride sunulmuştur.

1.5.1. Bilgi Toplama Araçları

Bir saldırganın bir saldırı başlatmadan önce attığı ilk adım, saldırının başlatılacağı ortamı anlamaktır. Bunu yapmak için saldırganlar tarafından başlangıçta ağ sayısı, bilgisayar sayısı, bilgisayar çeşitleri, işletim sistemleri, yazılım sistemlerinin sürümleri vb. bilgileri toplamaktadır. İlgili bilgiler toplandıktan sonra, çeşitli araçlar kullanarak hedef web sayfası veya ağın zayıf noktaları istismar edilmeye çalışılmaktadır. Bilgi toplama araçları (Hoque ve ark., 2013), iki kategori altında; algılama ve tarama araçları olarak incelenecektir.

1.5.1.1. Algılama Araçları

Etkili bir algılama aracı ağ üzerinde bulunan paketleri yakalama, inceleme, analiz etme ve görselleştirme özelliklerine sahip olmalıdır. Bu tür araçlar daha sonra kullanılacak olan ek paket özelliklerinin çıkarılmasına da yardımcı olmaktadır. Çoğu algılama aracı temel protokol parametrelerini kullanarak görselleştirmeyi ve ağ yapısının anlaşılmasını kolaylaşmaktadır. Bazı popüler algılama araçları aşağıda açıklanmaktadır.

a) Tcpdump: Güvenlik uzmanları için önde gelen paket analiz aracıdır. Ağ yöneticisine paket verilerini yakalama, kaydetme ve görüntüleme olanağı

sağlamaktadır. Bu araç, Wireshark gibi üçüncü parti yazılım tarafından da kullanılabilir.

b) Ethereal: Çok platformlu bir algılayıcı ve trafik analizörüdür. GTK+ ve GUI tabanlı bir kütüphane ile paket yakalama-filtreleme kütüphanesi olan libpcap vardır. Ethereal, tcpdump verilerini okuyabilir ve koşullu olarak kayıtları seçerek görüntülemek için tcpdump filtreleri uygulayabilmektedir. Bu araç ağ saldırısını belirleme ve denetleme konusunda faydalıdır.

c) Net2pcap: Paket trafiğini Pcap dosyasına dönüştürmek için kullanılan basit bir araçtır. Dönüşüm sırasında herhangi bir kütüphane kullanmaz. Linux Kütüphanesi olan LIBC'yi kullanır. Saldırı sırasında trafiği yakalar ve analiz edebilir.

d) Snoop: Tcpdump'a çok benzeyen bir Linux aracıdır. Dosya biçimi olarak PCAP değil de RFC 1761'i kullanmaktadır. Paket verilerinin filtrelemesi, okuması ve analiz edilmesine izin vermektedir.

e) Angst: Linux ve OpenBSD tabanlı aktif bir paket algılayıcısıdır. Ağa veri enjekte ederek veri yakalamasına olanak tanır.

f) Ettercap: Birden fazla platformu destekleyen etkili bir algılayıcıdır. Ettercap, aktif bir saldırı aracı olarak da kullanılmaktadır. NCURSES arabirimini kullanmaktadır.

g) Dsniff: Aktif bir ağda algılama yapabilen araç koleksiyonudur. Bu araç SSHv1 ve HTTPS oturumlarında ortadaki adam (man-in-the-middle) saldırılarına karşı etkilidir.

h) Cain&Able: Windows işletim sisteminde çalışan çok amaçlı bir algılama aracıdır. Bazı protokoller için şifre kurtarma işlemine izin verir. Bu araç SSHv1 oturumunda ortadaki adam saldırılarına karşı etkilidir.

ı) Tcptrace: TCP bağlantı bilgilerini tespit ederek gösterebilmektedir. Tcptrack, ağ arabirimindeki bağlantıları pasif olarak izleyebilir, durumlarını takip edebilir ve bağlantı listesini görüntüleyebilmektedir. Kaynak IP, kaynak bağlantı noktası, hedef IP, hedef bağlantı noktası, bağlantı durumu ve bant genişliği kullanımı gibi bilgileri görüntüleyebilmektedir.

i) Nstreams: Ağ dışına çıkan bilgileri görselleştirerek analiz edebilen bir araçtır. Bu araç isteğe bağlı olarak IPCHAINS veya IPFW kurallarına uygun çıktılar verebilir. Tcpdump komutlarıyla verilen çıktıları ayrıştırabilmektedir.

j) Argus: Bu araç farklı işletim sistemlerinde çalışabilmekte, paket verilerini veya yakalanan trafik dosyalarını işleyebilmektedir. Paket akışı sırasında algılanan bilgileri durum raporu olarak verebilmektedir.

k) Karpski: Sınırlı algılama ve tarama özelliklerine rağmen kullanıcı dostu bir algılama aracıdır. Bu araç, yerel bir ağdaki adreslere karşı bir saldırı başlatma aracı olarak da kullanılmaktadır.

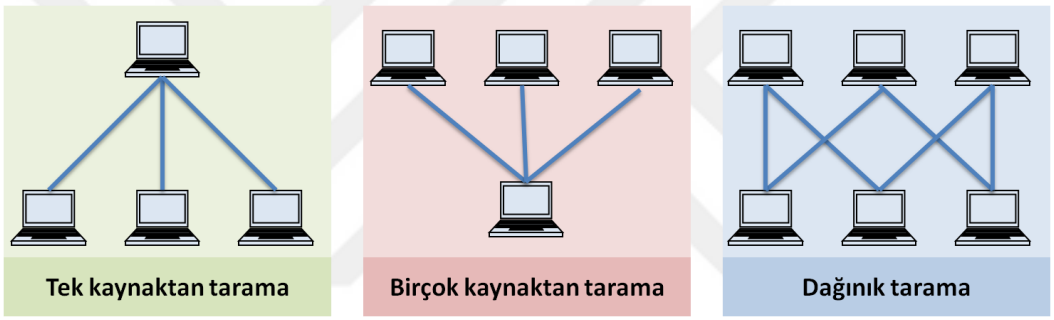
l) Aldebaran: Gelişmiş özelliklere sahip LIBPCAP-tabanlı TCP protokolünü algılama ve filtreleme aracıdır. Bu araç flag ayrıntıları olmadan kısmi header bilgileri sağlayabilmektedir. Ayrıca, paroları algılamak için bağlantılarla gönderilen verileri izler. Paket üstbilgilerini ve yük içeriğini algılamak için libpcap kurallarını kullanır ve yakalanmış verileri UDP vasıtasıyla başka bir ana makineye iletebilir. Buna ek olarak istenilen paket istatistiklerini şifreleme, analiz etme ve raporlama özelliklerine sahiptir.

m) ScoopLM: LM ve NTLM kimlik doğrulama bilgilerini yakalamak için Windows işletim sistemi tabanlı bir algılayıcıdır. Yakalanan veriler kimlik doğrulama sistemini geçmek için BeatLM kullanılmaktadır.

Algılama araçları farklı amaçlar doğrultusunda kullanılmak üzere tasarlanmıştır. Dolayısıyla ağ güvenlik uzmanı veya saldırgan kendi gereksinimleri eldeki görevle olan ilgisi, önemi ve etkinliğini değerlendirerek bu araçları kullanılır. Örneğin; Cain & Able şifre kırma yeteneğine sahipken ağ trafiğini yakalamak için uygun değildir. Benzer şekilde paket içindeki tüm bilgileri yakalamak ve bir dosyaya kaydetmek için Tcpdump ve Libpcap kullanılır. Öte yandan Gulp paket trafiği yakalama için çok kullanışlı olsa da Netflow yakalamada kullanılamaz şeklinde örnekler verilebilir.

1.5.1.2. Ağ Tarama Araçları

Ağ güvenlik uzmanı ve saldırgan içinde önemli olan bir konuda ağın taranması ve ağ mimarisinin çıkartılmasıdır. Ağ tarama aracı kullanılarak ağdaki aktif makineler belirlenebilmektedir. Ağ taraması ile elde edilen bilgiler analiz edilerek ağ açıklıkları tespit edebilmektedir. Etkili ağ tarama araçları farklı bağlantı noktaları konfigürasyonuna göre çalışma yöntemleri Şekil 1.28.'de gösterilmiştir. Bu tür bir ağ tarama aracı; ana bilgisayar, port ve IP adresleri hakkında genel bir durum raporu sağlamaktadır. Yaygın olarak kullanılan tarama araçları, özellikleri ve kaynakları anlatılacaktır.



Şekil 1.28. Bağlantı noktası tarama çeşitleri

a) Nmap: Ağın taranması ve güvenlik denetiminin yapılmasını sağlar. Hızla bir şekilde ağ tarama yeteneğine sahiptir. IP paketleri ile ana bilgisayar tarafından sunulan hizmetleri, işletim sistemlerini, paket filtreleri ve güvenlik duvarları gibi birçok kullanışlı parametreyi etkin bir şekilde tanımlayabilir. Nmap, sadece ağ parametrelerini taramak ve toplamak için değil, aynı zamanda ağ denetimlerini yapan ağ envanterin korunması, servis güncelleme çizelgelerinin yönetimi kullanıcıların çalışma süresinin izlenmesi gibi diğer rutin görevlerini de yerine getirebilmektedir.

b) Amap: Bu araç, genellikle uygulama protokolünün el sıkışması için tetikleme paketleri gönderen ve belirli bir port'da çalışan uygulamaları tespit edebilmektedir. TCP veya UDP bağlantı noktalarına bağlı kalmadan uygulama protokolünü algılama yeteneğine sahiptir.

c) Vmap: Sahte komutlara verdiği yanıtlara dayanarak bir sunucunun sürümünü belirleyebilmektedir.

d) Unicornscan: Asenkron ağ tarama aracıdır. Ölçülebilir bilgileri hızlı bir şekilde toplamaktadır. TCP/IP yapısı kullanır ve ağadan bilgiler almak için kullanıcı dostu bir ara yüze sahiptir.

e) Ttlscan: Ana makinenin her bağlantı noktasına TCP SYN paketleri gönderir, LIBNET ve LIBPCAP özelliklerini kullanarak ana makineyi tanımlar. Ana bilgisayardan gelen yanıtı ile bu paketlerin güvenlik duvarı arkasındaki başka bir ana makineye ileterek servisleri barındıran kimlikleri belirlemek için kullanır. Güvenlik duvarının arkasındaki ana bilgisayarda çalışan işletim sistemi sürümlerini tanımlamak için TTL, pencere boyutu ve IPID gibi belirli üstbilgi parametrelerini kullanır.

f) Ike-scan: Bu araç IKE protokolüne dayalı olarak IPSec VPN sunucularını keşfedebilir ve test edebilmektedir. Ike-scan, Linux, Unix, Mac OS ve Windows ortamlarında GPL lisansı altında çalışmaktadır.

g) Paketto: TCP / IP ağlarının manipüle edilmesine yardımcı olmak için geleneksel olmayan stratejiler kullanmaktadır.

Büyük bir ağ taraması için Nmap'in en iyi seçim olduğu düşünülebilir. Bu araç, yalnızca büyük bir ağ taraması için çeşitli seçenekler sunmakla kalmaz aynı zamanda bilgisayar portlarını, işletim sistemlerini, protokollerini, performansını, güvenlik duvarı değerlendirmesini ve sızdırmayı belirleme özelliklerini de belirleme yeteneğine sahiptir. Çoğu ağ yöneticisinin kullandığı çok popüler ve özellikli bir araçtır. Amap ve Vmap benzer araçlar olmasına rağmen, Nmap'ın işlevlerinin çoğunu destekleyemez. Çoğu DDoS saldırganı, saldırılarını yönetmek için kullandığı C&C sunucunda kullanılacak köle bilgisayarları bulmak için, bilgisayarın güvenlik açığını Namp aracı kullanarak elde eder.

1.5.2. Saldırı Başlatma Araçları

Son yıllarda çeşitli düzeylerde gelişmişliğe sahip çok sayıda saldırı başlatma aracı ortaya çıkmış ve web sitelerinden kolayca elde edilebilmektedir. İsteyen herkes bu araçları kolayca indirebilir ve bunları kötü amaçlı etkinlikler için kullanabilir Saldırı başlatma araçları; Truva atları, ağ katmanı saldırı araçları ve uygulama katmanı saldırı araçları olacak şekilde üç ana kategoride incelenecektir.

1.5.2.1. Truva Atları

Truva atı (Trajon) olarak adlandırılan virüsler, bilgisayardaki dosyaları veya ağın güvenlik sistemini bozacak kadar güçlü kötü amaçlı dosyalardan oluşmaktadır. Kullanıcının bir dosyayı açmaya çalışması ile aktif hale gelen Trojan'lar bu sayede zararlı faaliyetler gerçekleştirme alanına sahip olurlar. Trojan dosyaları genellikle internet, web sayfaları, sahte oyun programlarından bulaşmaktadır. Truva atlarının yedi farklı türü vardır.

a) Uzaktan Erişimli Truva Atları: Bu tür zararlı yazılım programları hedef makinede yönetici ayrıcalığını kontrol etmek için arka kapı olarak adlandırılan kullanıcının bilgisi olmadan işlem yapma özelliğine sahiptirler. Kullanıcı, oyun programı veya e-posta talebi ile bu tür Truva'yı farkında olmadan indirebilir. Saldırgan makineyi ele geçirdikten sonra Trojan sayesinde, söz konusu bilgisayarı DoS veya DDoS saldırısında kullanmak üzere BOTNET'e dahil eder. Bu tür Trojanlara örnek olarak "Danger" verilebilir.

b) Trojan Gönderen: Çok tehlikeli bir Trajon türüdür. Saldırgana hedef hakkında gizli bilgiler verebilmektedir. Kullanıcının klavye kullanırken kaydedilen tuş bilgilerini, banka şifrelerini, kredi kartı bilgilerini, e-posta adreslerini ve kişisel sohbet yazışmaları gibi hassas bilgileri kaydederek saldırgana ileten bir keylogger kurar. Bu tür Trojanlara örnek olarak Badtrans.B ve Eblast verilebilir.

c) Zararlı Truva Atları: Bazı önemli programları yapılandırabilen ve DLL dosyalarını otomatik olarak silerek bilgisayara bulaştıracak şekilde programlanmış tehlikeli bir tür Trajon'dur. Böyle bir Truva, uzaktan yönetilebilir ve önceden programlanmış talimatları zamanı geldiğinde uygulayabilir. Örnek olarak Bugbear ve Goner verilebilir.

d) PROXY Truva Atları: Hedef bilgisayarı PROXY sunucusu olarak kullanmaya çalışmaktadır. PROXY Trajon'larına örnek TrojanPROXY:Win32 ve Paramo.F verilebilir.

e) FTP Trojanları: Bu Trajon türü, Dosya Aktarım Protokolü (FTP) 21'nci port'unu açarak dosya kurulumu yapmaya çalışır. FTP Trojanuna örnek FTP99cmp'dir.

f) Güvenlik Yazılımını Devre Dışı Bırakan Trajon: Bu tür Trajonlar, virüsten koruma programları veya güvenlik duvarları gibi mekanizmaları yok edebilecek kadar güçlüdürler. Örnek olarak Trojan.Win32.KillAV.ctp ve Trojan.Win32. Disable.b verilebilir.

g) DoS Trojanları: DOS maksadıyla kullanılan Trajon çeşididir. Örneğin Ping-of-death ve Teardrop bu tür bir Trajon'dur.

1.5.2.2. Ağ Katmanı Saldırı Araçları

DoS bir hizmetin meşru kullanıcılarının istenen kaynakları kullanmasını engellemek amacıyla, bir saldırgan tarafından açıkça yapılmaya çalışılan girişimdir. DDoS ise DOS saldırısının farklı birçok noktadan yapılarak hedef sistemin ağ kaynaklarının kullanılabilirliği istismar etme konusunda koordine edilmiş bir girişimdir. Birçok DoS ve DDoS saldırı aracı geliştirilmiş ve herkes tarafından

kolayca erişilebilir ve kullanılabilir hale gelmiştir. Bu araçlardan bazıları ve özellikleri aşağıda sunulmuştur.

a) Jolt: Bu araç, Windows 95 veya NT işletim sistemlerinde çalıştıran hedef makinede, çok sayıda parçalanmış ICMP paketi göndererek saldırır. Hedef makine bunları yeniden birleştirmeyi başaramaz ve sonuç olarak klavye ve mouse işlem yapamaz hale gelir, yani bilgisayar donar. Bu aracın neden olduğu hasar çok ciddi değildir ve basit bir yeniden başlatma ile bu saldırıdan kurtarılabilir.

b) Bubonic: Çok sayıda TCP paketi göndererek Windows 2000 işletim sistemini kullanan bilgisayarlara saldırabilir. Hedef makinedeki yük önemli derecede artar ve herhangi bir girişi kabul etmez duruma gelerek sistem çöker.

c) Targa: 16 farklı DoS saldırı programından oluşur. Bu saldırıları tek tek veya gruplar halinde başlatabilir.

d) UDPFlood: IP adreslerinin belirli portlarına UDP paketleri göndererek saldırı yapabilir. Bu araç ayrıca bir sunucunun performansını test etmek için de kullanılabilir.

e) FSMax: Sunucu stres test aracıdır. Bir saldırıyı gerçekleştirirken kullanılabilecek arabellek taşmasını sınamak için bir metin dosyasını girdi olarak kabul eder ve sunucunun yeteneğini değerlendirir.

f) Nemsey: Bu aracın varlığı o bilgisayarın güvensiz olduğu ve kötü niyetli yazılımların bulaştığını gösterir. Protokol ve bağlantı noktası gibi bilgiler dâhil olmak üzere saldırgan tarafından belirlenen sayıda paket içeriğini bir saldırıyı başlatmada kullanabilir.

ı) Panter: UDP tabanlı DoS saldırı aracıdır.

g) Slowlowis: Kısmi talep göndererek hedef Web sunucusuna çok sayıda bağlantı oluşturur ve bunları uzun süre açık tutmaya çalışarak saldırı başlatır.

h) BlackEnergy: HTTP tabanlı bir BOTNET'dir. Ayrıca Web ara yüzünü kullanan IRC tabanlı C&C sunucusuna sahip bir DDoS saldırı aracıdır.

ı) HOIC: HTTP Flooding saldırısı oluşturmaya odaklanan çok etkili bir DDoS aracıdır. Aynı anda 256 web sitesine saldırabilir.

i) Knight:: IRC tabanlı olan bu araç, windows işletim sistemini kullanan bilgisayarlara birden fazla UDP Flooding DDoS saldırısı başlatabilir.

j) Kaiten: UDP ve TCP flooding, SYN ve PUSH+SYN çoklu saldırılarını başlatabilen IRC tabanlı bir saldırı aracıdır. Rastgele kaynak adresleri kullanır.

k) LOIC: IRC ile çalışan çok etkili bir DDoS saldırı aracıdır. Birden fazla protokolü destekler ve üç farklı saldırı modunda çalışır. TCP, UDP ve HTTP.LOIC saldırı başlatmak için kullanır.

l) Hgod: Windows XP tabanlı bu araç saldırıda kullanılacak IP adresleri, port numaraları ve protokolleri belirtmek için kullanılır. TCP SYN Flooding saldırısını kullanılır.

DoS/DDoS saldırı araçlarının geniş ve sürekli artan bir havuzundan yalnızca seçilmiş birkaçı tanıtılmıştır. Çoğu saldırı aracına internetten kolayca erişilebilir. Bununla birlikte, bunlar arasında LOIC ve HOIC, kısa süre içinde bir DDoS saldırısı başlatmada çok etkilidir. LOIC, TCP, UDP ve HTTP protokollerini içeren saldırı paketleri üretebilir. Ayrıca bu araçların kamuya açık bir ağda saldırı başlatmak için kullanılması etik olmadığı gibi kanunlar önünde suç teşkil eder.

1.5.2.3. Uygulama Katmanı Saldırı Araçları

Uygulama katmanı DDoS saldırıları genellikle düşük hız DDoS saldırılarıdır ve meşru protokolleri ve meşru bağlantıları kullandıkları için ağ katmanı saldırılarına göre daha akılcı ve çözümü zordur. Bu nedenle uygulama katmanı saldırılarının tespit edilmesi çok zordur. Bir uygulama katmanı saldırı aracı genellikle meşru olarak bağlı olan ağ makinelerinden meşru HTTP isteklerini bir web sunucusunu bağlanmak için kullanır (Xie ve Yu, 2009). Uygulama katmanı saldırıları dört temel kategoride incelenecektir.

a) HTTP ile ilgili saldırılar: Bu tür uygulama katmanı saldırısında, saldırgan, hedef siteyi çok kısa bir sürede bastırmak için çok sayıda HTTP isteği gönderir. Örnek olarak Nimda ve AppDDoS'dur.

b) SMTP ile ilgili saldırılar: Bu saldırıda, saldırgan internet üzerinden SMTP protokolünü kullanarak e-posta saldırısı göndermektedir.

c) FTP ile ilgili saldırılar: Bu saldırıda, saldırgan hedefe meşru FTP bağlantısı kurar ve saldırı paketlerini gönderir.

d) SNMP ile ilgili saldırılar: Bu tür saldırıda, sistemin yapılandırmasını değiştirmeyi ve sistem durumu veya kullanılabilirliğinin izlenmesi amaçlamaktadır.

1.5.3. Ağ İzleme Araçları

Ağ yöneticileri için; ağ trafiğini izlemek, oluşan anomaliyi gözlemlemek, analiz etmek ve tanımlamak çok önemli bir faaliyettir. Bir sistemin gizlilik, bütünlük ve erişim denetimi mekanizmalarından ödün vermemek veya bir hizmetin meşru kullanıcılarının istenen kaynaklara erişmesini sağlamak ve kötü niyetli girişimlerin ağ trafiğini görselleştirmek bu tür faydalı araçlar ile yapılmaktadır.

1.5.3.1. Görselleştirme ve Analiz Araçları

Ağ yöneticisinin mevcut ağ trafiğini izleme ve analiz edebilmesi için etkili bir ağ trafiği görselleştirme aracına ihtiyacı vardır. Uygun bir görselleştirme ile analiz sonuçlarının anlamlı bir şekilde yorumlanmasın desteklemekle kalmaz, aynı zamanda sistem yöneticisine anormallik kalıplarını tanımlanmasında yardımcı olur. Bazı görselleştirme araçları aşağıda sunulmuştur.

a) Tnv: Ana bilgisayar ve yerel bilgisayarlar arasındaki ağ paket ayrıntıları ile zamana dayalı trafik görüntülemesini yapar. Tnv, bir ağdaki normal kalıpları öğrenmeye, paket ayrıntılarını araştırmaya ve ağda sorun gidermeye yardımcı olur.

b) Network Traffic Monitor: Ayrıntılı ağ trafiğinin taranması ve görselleştirilmesini sağlar. Trafik detaylarının analiz edilmesine izin erir.

c) Rumint: Windows işletim sistemli tabanlı bu araç, kaydedilmiş PCAP trafik verisi ve mevcut ağ trafiğinin görselleştirmesini yapar.

d) EtherApe: Unix işletim sisteminde yakalanan verilerin izleyebilmesini sağlayan bir araçtır.

e) NetGrok: Ağ verisinin görsel şemasını harita olarak grafiksel bir düzende oluşturan etkili bir gerçek zamanlı ağ izleme aracıdır.

f) NetViewer: Yakalanan gerçek zamanlı trafik verilerini toplu olarak gözlemlenmesine yardımcı olmakla kalmaz aynı zamanda ağ anomalilerini tanımlanmasında etkili bir görselleştirme aracıdır.

g) VizNet: Bir ağın bant genişliği kullanımına dayalı olarak performansını görselleştirmeye yardımcı olur.

2. GEREÇ VE YÖNTEM

2.1. Verilerin Analizi

DDoS saldırı araçları ve yöntemlerinin gelişmesi sonucu DDoS saldırısı tespiti ve önlenmesi için birkaç yeni ve pratik makine öğrenme yaklaşımı geliştirilmiştir. Bu yöntemlerin önemi ve etkinliği; sınıflandırma doğruluğu ve süreç performanslarına dayanır. Bu yaklaşımlar, istatistiksel, bilgi temelli, yumuşak hesaplama tabanlı ve diğer veri madenciliği ve makine öğrenme yaklaşımları olmak üzere dört temel kategoride incelenmiştir (Bhattacharyya ve Kalita, 2013). Bu çalışmada özellikle mobil BOTNET'lerin tespitinde kullanılacak olan Mobil BOTNET ortak özellikleri incelenmiş ve bilgi temelli yaklaşım kullanılmıştır.

2.2. Gereçler

Bir uygulamanın işlemini, yapısını ve işlevlerini öğrenmek amacıyla uygulamanın tekrardan kaynak kodlarına ulaşılmasına tersine mühendislik denmektedir. Bu yöntem; uygulamanın algoritması ve kaynak kod içinde kullanılan komutların incelenmesine imkân vermektedir. ANDROID işletim sisteminde kullanılan APK dosyaları için de tersine mühendislik tekniği kullanılmaktadır. APK dosyalarının tersine mühendislik tekniği ile orijinal uygulamanın kaynak koduna; ApkTool, Dex2Jar, Notepad++, AndroGuard vb. araçlar ile ulaşılmıştır.

2.3. Yöntem

Çalışmanın amacında belirtilen hipotezleri test etmek için BOTNET saldırılarının ortak özelliklerini belirlemek için, son yıllarda yaygın ve en çok aktif olan ZtorgB.Gen, Lop.c, Muetan.b, Zitmo, TigerBot, AnServerBot, Geinimi, PjApps, RootSmart/Bmaster, DroidDream, DroidKungFu, SMSpacem, FakePlayer, ADRD, Spy.Banker.HU, BaseBridge ve Nickispy BOTNET saldırıları incelenmiştir. Analiz edilen MALWARE örnekleri Contagio Kütüphanesinden indirilmiştir.

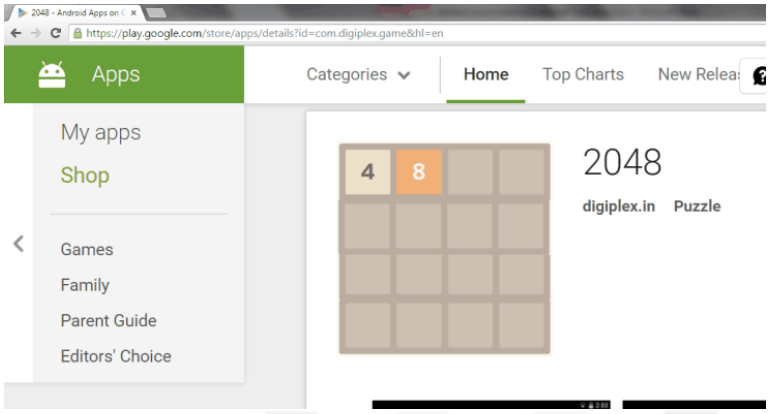
2.4 Mobil BOTNET Uygulaması

Mobil BOTNET'lerin temel kaynağı zararlı yazılım monte edilmiş ve üçüncü parti uygulama sayfaları tarafından kullanıcılara bulaştırılarak ele geçirilmiş akıllı cihazlardır. Bu bölümde basit bir ANDROID uygulamasına zararlı yazılımın nasıl entegre edildiği ve DDOS veya farklı amaçlarla nasıl kullanıldığı anlatılmaktadır. Burada anlatılanlar sadece zararlı yazılım nasıl oluşturulduğu konusunda bilimsel bilgi verilmektir. Virüslerin nasıl yazıldığı veya yayılma yöntemleri ile ilgili kanun dışı bilgiler verilmemektedir.

Uygulama aşamaları;

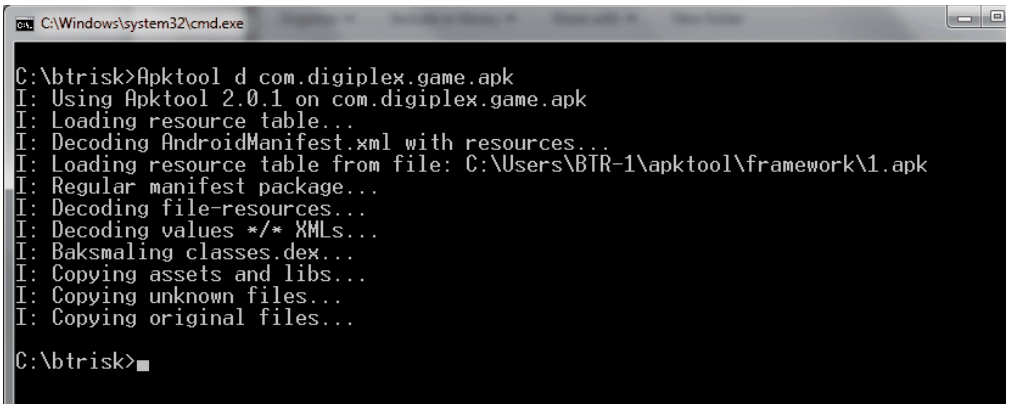
- Zararlı yazılım monte edilecek olan ANDROID uygulamasının seçilmesi,
- APK uygulamasındaki dosyaların Cleartext formatına dönüştürülmesi,
- Classes.Dex dosyasında bulunan derlenmiş kodlar elde (Decompile) edilmesi,
- Manifest.xml dosyasında zararlı kod ve izinlerin tanımlanması,
- Zararlı yazılımın APK uygulamasına yerleştirilmesi,
- Zararlı kod içeren APK uygulamasının derlenmesi (Compile) edilmesi,
- Uygulamanın imzalanarak hedef cihazda çalıştırılması şeklinde tasarlanmıştır.

Hedef uygulama olarak basit bir oyun uygulaması seçilmiştir. Seçilen uygulamaya ait ekran görüntüsü Şekil 2.1'dedir.



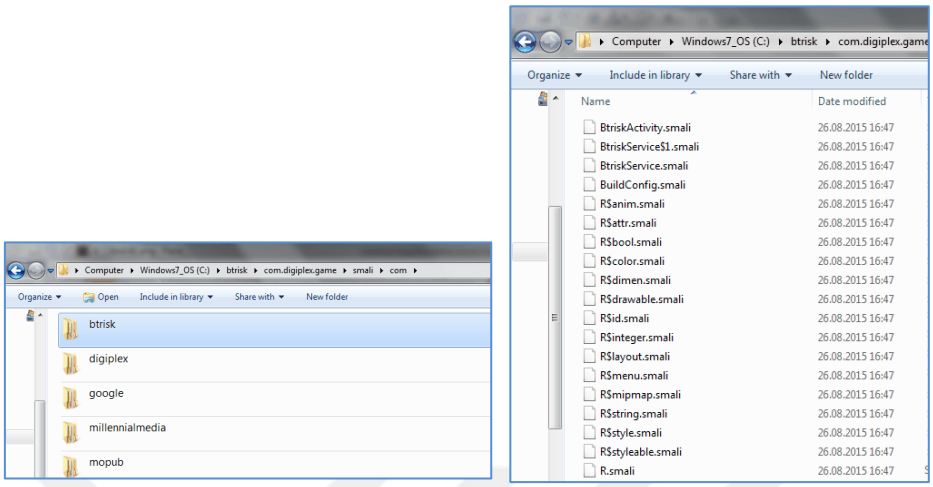
Şekil 2.1. Hedef uygulama

İlk adım olarak uygulama Apktool aracı ile DECOMPILE edilerek dosyaları okunabilir hale getirecektir. DECOMPILE ekran görüntüsü Şekil 2.2'de verilmiştir. (Btrisk, 2017).



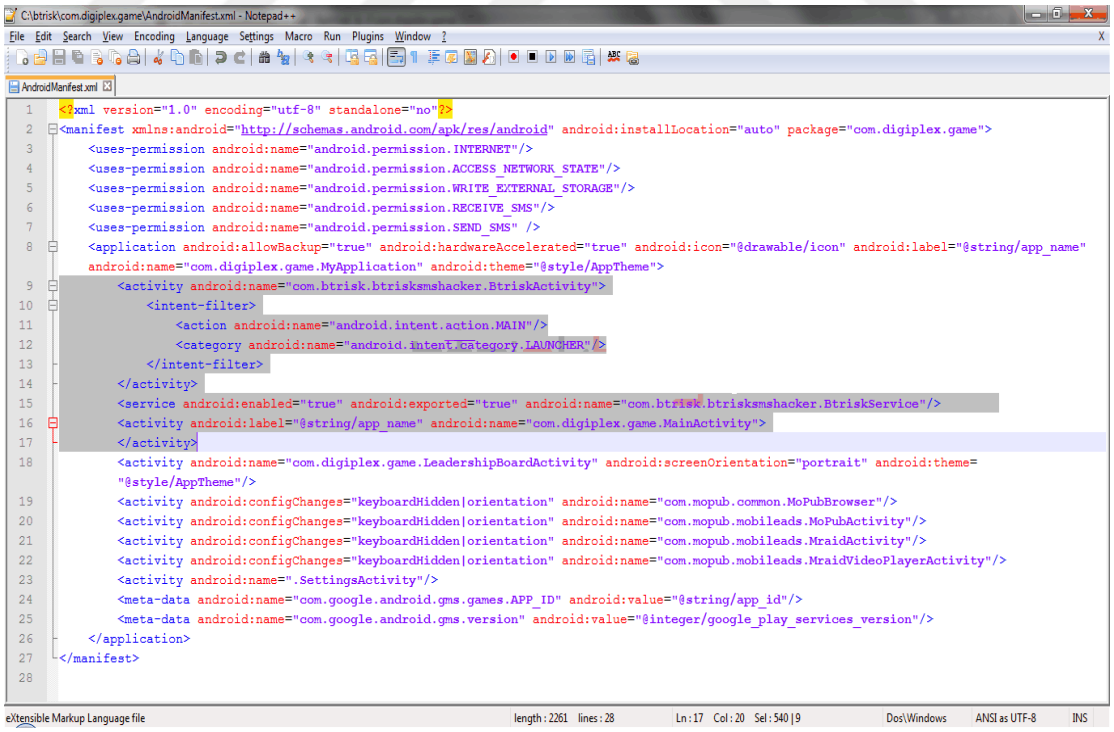
Şekil 2.2. APKTool aracının kullanımı (Btrisk, 2017).

DECOMPILE edilen uygulamaya ait dosyalar artık Windows işletim sistemi ile açılabilmekte ve üzerinde değişiklik yapma imkanı sunmaktadır. BTRISK olarak hazırlanan zararlı kod içeren yazılım Şekil 2.3'de gösterilen klasörlerin içine kopyalanmaktadır (Btrisk, 2017).



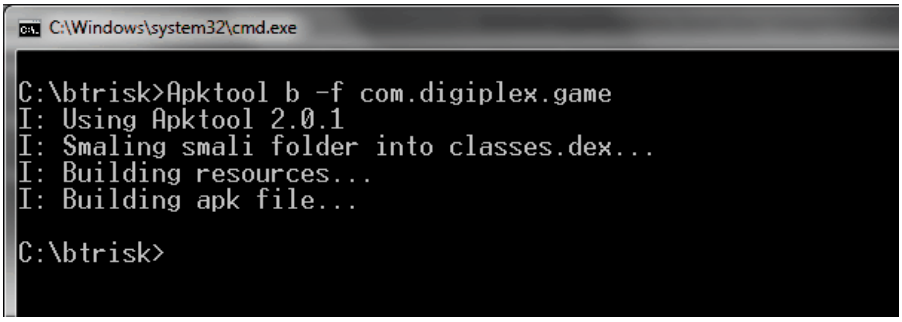
Şekil 2.3. Zararlı yazılım dosyaları (Btrisk, 2017).

Daha sonra zararlı yazılım yerleştirilen uygulama ait AndroidManifest.xml dosyasını Şekil 2.4 uygun olarak düzenlenmektedir.



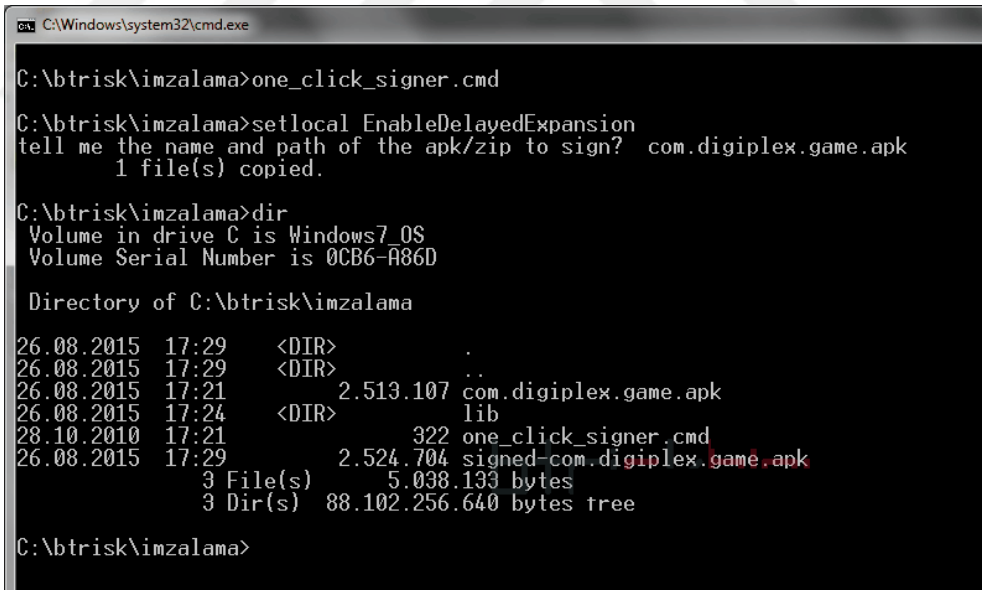
Şekil 2.4 AndroidManifest.xml Dosyasını Düzenlenmesi (Btrisk, 2017).

Zararlı yazılım yerleştirilen uygulama tekrardan APK uygulama formatına çevrilmesi için Şekil 2.5'de gösterildiği gibi tekrardan COMPILE edilmektedir.



Şekil 2.5. APK uygulamasının COMPILE edilmesi (Btrisk, 2017).

Son olarak da zararlı yazılım entegre edilen yazılım imzalanarak Mobil BOTNET olarak kullanıma hazır hale getirilmektedir. Komut işlemleri Şekil 2.6'da sunulmuştur.



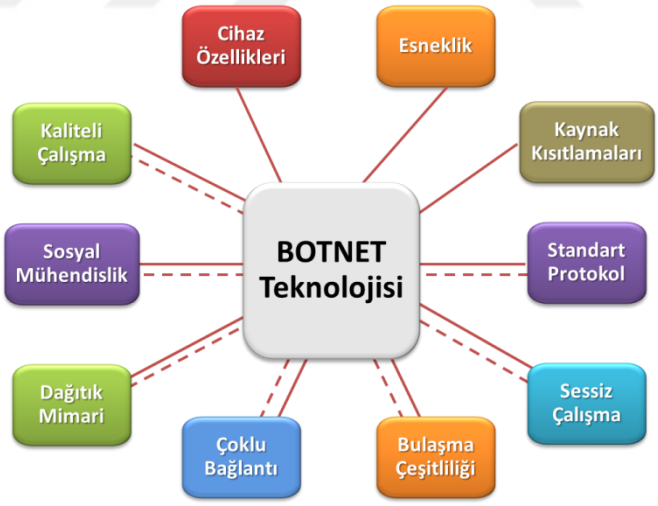
Şekil 2.6. Zararlı yazılım içeren APK dosyasın imzalanması (Btrisk, 2017).

Yazılım kurulan akıllı cihaz artık bir Mobil BOTNET'de DDOS saldırısı veya farklı zararlı amaçlar için kullanıma hazır hale gelmiştir.

3. BULGULAR

3.1. BOTNET Hakkında Genel Değerlendirme

Geleneksel BOTNET kullanarak etkili bir DDoS saldırısı başlatma aracı tasarımı gereksinimlerinin, mobil BOTNET için olanlardan çok farklı olmadığı görülmektedir. Mobil BOTNET tabanlı saldırı başlatma aracı, sınırlı bant genişliği, sınırlı batarya kapasitesi, merkezi güvenlik yönetimi eksikliği, geleneksel BOTNET kıyasla güvenlik duvarı korumasının olmaması nedeniyle saldırganlar için daha elverişli koşullar oluşturmaktadır. BOTNET tasarımını etkileyen başlıca faktörler Şekil 3.1'de sunulmuştur. Geleneksel BOTNET tasarımı için önemli konular kesik çizgilerle gösterilmiş, mobil BOTNET tasarımı için sorunlar düz çizgilerle ifade edilmiştir.



Şekil 3.1. BOTNET tasarımını etkileyen başlıca faktörler

Tek bir BOT'un başarısızlığı tüm ağ üzerinde çok fazla etkisi yoktur. BOTNET teknolojisinde, uzaktan yönetim komutlarının ara birim sunucularına iletilmesi durumunda, güvenlik uzmanlarının BOTNET denetleyicilerinin tanımlanmasını ve

saldırı yoğunluğunun belirlenmesinde zorlanmaktadır. Ayrıca, amaç yüksek seviyede zarara uğratmak ise, sadece BOTNET saldırı yoğunluğunu arttırmak daima etkili olamaz. Artan boyut BOTNET'in görünürlüğünü arttırır. Nispeten küçük bir boyutta, örneğin 15000 ila 20000 BOT üyesi olan bir BOTNET, birleşik bant genişliği uygun becerili kodlama ile doğru bir şekilde kullanılabilirse, hedef web sitesine veya sunucusuna zarar vermede oldukça etkili olabilir.

BOTNET teknolojisindeki hızlı gelişmeler ve akıllı telefonların artan kullanımı ile mobil BOTNET'ler, SPAM SMS, DDoS saldırısı ve reklam tıklama sahtekârlığı gibi hücresel ağ saldırıları başlatması için etkili bir platform olarak ortaya çıkmaktadır. Geleneksel BOTNET'lerin aksine, mobil BOTNET tasarımı, cihaza özgü kaynak kısıtlamaları (ör. Pil kapasitesi, CPU gücü vb.) ve esneklik faktörlerinden etkilenir. Mobil BOTNET'lerin tasarımında bu faktörler dikkate alınmaktadır. Dahası akıllı telefonlar bir saldırıya karşı daha savunmasızdır, çünkü bir SMS komut ve kontrol sistemi veya Bluetooth (Zeng ve ark.,2012) yoluyla bir cep telefonuna erişmek kolaydır. Ayrıca P2P topolojisi sayesinde mobil BOT'ların P2P tarzında komut almasına olanak tanınmakta ve tespiti daha da zorlaşmaktadır. Saldırı planlayıcıları ve tasarımcılar ayrıca, iletişimin içeriğini gizlemeye yardımcı olduğu için mobil BOTNET iletişiminde HTTP kullanımını tercih etmektedirler.

3.2. DDoS Savunma Sisteminde Olması Gereken Özellikler

DDoS Savunma Sisteminin birincil amacı, sistemi canlı tutmak ve hedefin DDoS saldırısı altında olmasına rağmen meşru kullanıcılar tarafından ulaşılabilir kılmaktır. Bu nedenle, DDoS savunmasına yönelik aşağıdaki özelliklere sahip olması istenmektedir:

a) Gerçek Zamanlı Performans: Saldırının kötü amaçlı trafiği ile savunulan sistemin devre dışı kalmadan, muhtemelen yaklaşmakta olan bir saldırıyı tespit edebilmelidir.

b) Ölçeklenebilirlik: DDoS saldırılarının saldırı yoğunluğu yüzlerce Gbps olduğundan, algılama mekanizmasının zaman ve yoğunluk karmaşıklıklarını savunma sisteminin ölçeklenebilirliği açısından önemli rol oynamaktadır.

c) Hizmet Kalitesinin Korunması: Bir DDoS saldırısına karşı savunmanın önündeki en büyük engel, özellikle de düşük oranlı bir DDoS saldırısı durumunda, saldırının trafiğin içerikteki meşru trafiğinden ayırt edilemez olmasıdır. Dolayısıyla bir saldırıyı tespit etmek hedefin korunması için yeterli değildir. Normal trafiğin saldırı trafiğinden ayrılması için özel yöntemlere ihtiyaç duyulmaktadır. Böylece normal kullanıcıların hizmet kalitesi korunabilmelidir.

d) Kaynak Tanımlaması: Bir DDoS savunma sistemi saldırı kaynaklarını bulmak için IP Traceback ve Pushback mekanizmalarına sahip olmalıdır.

Cep telefonu ve mobil cihazlar; internet, konum belirleme sistemleri (GPS), kablosuz iletişim ve sağlık uygulamaları gibi ileri düzey yetenekler kazandırılmasıyla günlük hayatın her alanında kullanılır hale gelmiştir.

BOTNET ve DDoS saldırıları arasında doğrudan bir ilişki vardır. Tek bir IP'den yapılan saldırı çok çabuk ve basit bir şekilde IP adresinin yasaklanmasıyla engellenebilir. Ama bunun yüzbinlerce ve dünyanın çeşitli yerlerinden yapılan bir BOTNET saldırısı olarak orataya çıktığında, alınan emniyet tedbirlerinin çok güçlü olmadığı durumlarda saldırının amacına ulaşması anlamına gelmektedir. Amaçlanan servis dışı bırakma işlemi gerçekleşmiş olur. Siber silahın bir parçası olan DDoS ancak BOTNET ordusundaki BOT'ların sayısı ve çeşitliliği (PC, Akıllı Cihaz, IP Kamera, IoT vb.) ile güçlenmektedir.

2015 yılından sonraki DDoS saldırılarında kullanılan cihazların sadece köle bilgisayarların olmadığı, zararlı yazılım bulaştırılmış akıllı telefon, IP kamera, IoT ve internete bağlı cihazlarında bu siber silahın bir parçası olduğu tespit edilmiştir. Bu çalışmada, Mobil BOTNET saldırılarının tanımı, hâlihazırda mevcut BOTNET ailelerinin bir analizi ve DDoS maksadıyla kullanımı örnekler ile sunulmaktadır. Örnek olarak ele alınan zararlı yazılımlar (MALWARE) analiz edilerek, BOTNET saldırılarının ortak özellikleri ve davranışları açığa çıkarılmaktadır. Bu özellikler, ANDROID işletim sistemindeki yeni zararlı yazılımların tanımlanmasına yardımcı olacaktır. Bu sayede kullanıcı farkındalığının artması ve cihazları üzerinde gerekli güvenlik güncellemeleri ve resmi olmayan uygulama mağazalarından elde edilmiş yazılımları daha dikkatli kullanması sağlanacaktır.

3.3. Mobil BOTNET Geliştirme Modeli

Bir mobil uygulamanın zararlı yazılım içerip içermediğini veya BOTNET işlevlerine sahip olup olmadığını öğrenmek için, özellikleri algılama yöntemleri kullanılabilir. Şekil 3.2'de gösterilen Mobil BOTNET Geliştirme Modeli (BOTMASTER'ın bir BOTNET saldırısını geliştirme aşamaları) ve BOTNET saldırısının özelliklerinin hangi aşamalarda ortaya çıktığı anlatılmaktadır.

Şekil 3.2. Mobil BOTNET geliştirme modeli

BOTNET saldırısını oluşturulma süreci, BOTMASTER tarafından BOT koduna yer açmak için meşru bir uygulamayı değiştirerek Bulaşma Evresi ile başlar (Bailey ve ark., 2009). Tersine mühendislik; bir uygulamanın işlemini, yapısını ve işlevlerini öğrenmek amacıyla uygulamanın tekrardan kaynak kodlarına

ulaşılmasıdır. ANDROID uygulamaları için de tersine mühendislik tekniği kullanılmaktadır. BOTMASTER ilk önce tersine mühendislik tekniklerini kullanarak orijinal uygulamanın kaynak kodunu ApkTool, Dex2Jar, Notepad++, AndroGuard vb. araçlar ile elde etmektedir (Manjunath, 2011). Daha sonra orijinal uygulama kodlarına zararlı uygulama içerikleri ekleyerek orijinal yazılımdaki kodda değişiklikler yapmaktadır. Bu sayede birinci BOTNET özelliği olan Zararlı Yazılım Paketlenmesi gerçekleşmiş olur. BOTMASTER zararlı yazılım eklenmiş yeni uygulamanın cihazda çalışması için, AndroidManifest.xml dosyasında ilave izinlerin verilmesini sağlamaktadır. Bu dosyadaki herhangi bir değişiklik, sekizinci BOTNET özelliğini oluşturur.

Zararlı kodların uygulamaya başarılı bir şekilde bulaşmasından sonra, BOTMASTER yeni uygulamanın yayılmasını sağlamak için ikinci aşama olan Yayılma Evresine geçerek zararlı kod ile yeniden paketlenmiş bu uygulamanın dağıtımını sağlar. Böyle bir uygulamanın, diğer ANDROID cihazlarına yayılmaması ve BOTNET'in büyüme yeteneğini kaybetmesi durumunda hiçbir amaca hizmet edemez. Dolayısıyla zararlı kod ihtiva eden bu uygulama e-posta, dosya paylaşımı, üçüncü parti uygulama forum siteleri, ücretsiz veya zararlı URL'ler vasıtasıyla yayılmaktadır (Hachem ve ark., 2011). Ancak mobil cihazlarda BOTMASTER'ler için en yaygın ve en etkili aktarım ortamı üçüncü parti uygulama mağazaları ve forum siteleridir. ANDROID cihazlar için geniş bir üçüncü parti uygulama mağazası yelpazesi bulunmaktadır. Geliştiriciler, bu mağazalardaki uygulamalarını herhangi bir güvenlik politikası uygulamadan kolayca yükleyebilmektedir. Dolayısıyla BOTMASTER zararlı yazılım içeren yeniden paketlenmiş uygulamayı çoğaltmak için bir uygulama deposuna yükler. Bu aşama, yedinci BOTNET özelliğine (Üçüncü Parti Uygulama Mağazası) göstermektedir.

Mobil BOTNET Geliştirme Modeli'nin son aşaması, BOTNET'in amacına ulaşacağı Uygulama safhasıdır. Uzaktan Yönetim, Eposta ve SMS Okuma-

Gönderme, Veri Hırsızlığı, Ek İçerik İndirme/Kurma ve Kök Klasör Saldırısı gibi BOTNET'in diğer temel özellikleri bu safhada ortaya çıkmaktadır.

3.4. BOTNET Tespit Yöntemleri

BOTNET'in temel amacı; DDoS saldırısı, bilgi hırsızlığı, SMS veya harici bir sunucudan komutlar almaktır. Bu amacı gerçekleştirmesini engellemek için cihaz içindeki zararlı yazılımların tespit edilmesine ihtiyaç vardır. Uygulamaların zararlı yazılım içerip içermediğini belirlemek için tersine mühendislik yöntemi ve ANDROID izinlerinin analiz yöntemi incelenmektedir.

3.4.1. Tersine Mühendislik Yöntemi

Tersine mühendislik; bir uygulamanın işlemini, yapısını ve işlevlerini öğrenmek amacıyla uygulamanın tekrardan kaynak kodlarına ulaşılmasıdır. Bu yöntem; uygulamanın algoritması ve kaynak kod içinde kullanılan komutların incelenmesine imkân vermektedir. ANDROID işletim sisteminde kullanılan APK dosyaları için de tersine mühendislik tekniği kullanılmaktadır. APK dosyalarının tersine mühendislik tekniği ile orijinal uygulamanın kaynak koduna; ApkTool, Dex2Jar, Notepad++, AndroGuard vb. araçlar ile ulaşılmaktadır. BOTNET Keşif Süreci ise, bir güvenlik analistinin belirli bir uygulamanın BOTNET saldırıları ile ilgili olarak zararlı olup olmadığını belirlemek için izleyebileceği adımları açıklar (Pieterse ve Olivier, 2012). Tersine mühendislik sayesinde kaynak kodlarının her satırı incelenir ve zararlı yazılım içerip içermediği tespiti edilir. Ama güvenlik uygulamasının her kod satırını değerlendirmesi çok zaman alıcı bir iş olabilir. Ancak BOTNET ortak özelliklerinin, mobil BOTNET'in tespitinde kullanılması zararlı yazılım kodunun kolayca bulunmasına yardımcı olabilir.

3.4.2. ANDROID İzinlerini İnceleme Yöntemi

Olası zararlı uygulamaları bulmak için; mobil cihaza uygulama yüklendikten sonra, güvenlik analisti tarafından araştırılan uygulamanın yeniden paketlenmiş bir uygulama olup olmadığını belirlenmelidir (Zhou ve ark., 2012). Yeniden paketlenmiş uygulamalar, AndroidManifest.xml dosyasında tanımlanan izinler analiz edilerek; uygulama tarafından ortaya çıkabilecek olası tehditler tanımlayabilir. Aşağıda sunulan ANDROID izinleri, BOTNET tespiti için temel gösterge olarak kullanılabilir:

- INTERNET, ACCESS_NETWORK_STATE RECEIVE_BOOT_COMPLETED: Root yetkisi alabilir,
- INTERNET_RECEIVE SMS, SEND_SMS: Uzak sunucudan komut alabilir,
- ACCESS_WIFI_STATE, CHANGE_ WIFI_STATE: Cihazda değişiklik yapılabilir,
- INTERNET, READ_ PHONE_STATE, READ_CONTACTS: Cihaz bilgileri çalınabilir,
- İNTERNET, SEND_SMS: SMS gönderebilir,
- INTERNET, INSTALL_PACKAGES: Uygulama paketi indirebilir.

ANDROID izinlerinin bu alt kümelerini tanımlamak, bu izinlerin orijinal uygulamanın bir parçası olabileceğinden, bir tehdide atıfta bulunması gerekmez. Bununla birlikte, güvenlik analistinin tüm kod yapılarını değerlendirmek yerine yalnızca yukarıda belirtilen özelliklerle ilgili kodu taraması süreci kısaltmaktadır. BOTNET temel özellikleri, algılama mekanizmalarının incelenmesi ne kadar değerli olsa da, en güvenilir yöntem orijinal uygulama mağazalarından uygulamaların elde edilmesidir.

4. TARTIŞMA

Yapılan literatür araştırmasında DoS ve DDoS saldırılarının genel tanımı, amacı, hedefleri, hâlihazırda mevcut BOTNET ailelerinin DDoS maksadıyla kullanımı, türleri ve kullanılan araçlar hakkında birçok kaynağın mevcut olduğu görülmüştür. Son yıllarda yapılan araştırmaların birçoğu DDoS saldırıların algılama ve önleme sistemi üzerinde yoğunlaşmıştır. Ayrıca 2015 yılından itibaren mobil BOTNET'lerin DDoS maksadıyla kullanımları artmıştır.

Mirkovic ve ark. (2005a) tarafından DDoS saldırılarını sabit hız saldırısı, artan hız saldırısı, darbeli saldırı ve alt grup saldırısı olarak dört kategoriye ayırmıştır. Bu saldırı kategorileri ve kullanım zamanları ile ilgili yaklaşımlar geliştirilmiştir. Ayrıca kategorilere uygun algılama ve önleme sistemleri konusunda çalışmaları mevcuttur (Mirkovic ve ark., 2005).

Craig ve Ark., (2007) yaptığı çalışmada BOTNET ve DDoS saldırıları arasında doğrudan bir ilişkinin olduğunu ve çoklu bilgisayardan yapılan BOTNET saldırısının alınan emniyet tedbirlerinin çok güçlü olmasına rağmen etkili olabileceğini tespit etmiştir. DDoS ve BOTNET ordusundaki BOT'ların sayısı ve çeşitliliği PC, akıllı cihaz, IP kamera ve IoT ile güçlendiğini yakın geçmişte Agobot, Spybot, RBot ve SDBot gibi yeni BOTNET'lerin ortaya çıktığını ifade etmiştir (Craig ve Ark., 2007).

Mobil BOTNET varlığının keşfedilmesinden sonra yapılan çalışmalarda; zararlı yazılım özellikleri ve uygulama izinleri Joshi ve ark. (2015) ile Gorla ve ark. (2014) tarafından incelenmiştir. Joshi ve ark. (2015) zararlı yazılım özellikleri ve uygulama izinlerinin incelenmesi üzerinde yöntemler geliştirmiştir. BOTNET saldırıları arasındaki ortak özelliklerini belirlemek için izin tabanlı filtreleme

yaklaşımı kullanmıştır. Belirlenen bu özelliklerin, BOTNET temel özellikleriyle yakından ilgili olması sebebiyle ANDROID cihazlardaki BOTNET saldırılarının tespit edilmesinin mümkün olabileceği değerlendirmiştir (Joshi ve ark., 2015).

Gorla ve ark. (2014) çalışmasında ANDROID uygulama izin kullanımını analiz etmek için uygulama açıklamalarını ve kodlarını kullanmıştır. Önce uygulamaları, meta verilerini kullanımına göre sınıflandırmıştır. Aynı kümedeki uygulamaları API (Application Programming Interface) kullanımlarına göre analiz ederek diğer uygulamalarla kıyaslamış ve API yöntemlerini alışılmadık şekillerde kullanan uygulamaları şüpheli olarak işaretlemiştir. Bu çalışmada zararlı yazılım algılama oranları genellikle %60'ın altındadır. Ancak Joshi ve Gorla'nın çalışmaları sadece uygulama izinlerinin kontrolü ile sınırlı kalmış ve DDoS saldırılarının bir parçası olan zararlı yazılım bulaşmış mobil cihazlara karşı alınması gereken önlemlere çok fazla değinilmemiştir (Gorla ve ark. 2014).

Kılıç ve ark. (2016) çalışmasında; kullanıcıların kendi bilgisayarlarının DDoS saldırıları için köle bilgisayar olup olmadığının kontrolünün sağlanması doğrultusunda, üzerinde makine öğrenmesine dayalı sınıflandırma algoritmaları kullanarak köle bilgisayar tespiti yapılmıştır. Çalışma sonucunda, gerçek bir kullanım ağı ve köle bilgisayarda veri üreten bir araçtan elde edilen çıktılar üzerinde test edilen sınıflandırma algoritmaları arasında en iyi sonucu %93.58 doğruluk oranı ile Rasgele Orman algoritmasının verdiği gözlemlenmiştir. Kılıç ve ark. mobil cihazlar hakkında pek fazla önerilerde bulunmamıştır (Kılıç ve ark., 2016).

Hoque ve ark. (2015) çeşitli BOTNET mimarileri kullanılarak geliştirilen araçlar ve bu araçların artı ve eksileri hakkında ayrıntı bir analiz yapmıştır. Mobil BOTNET saldırılarının karakteristikleri ayrıntısı ile anlatılmıştır (Hoque ve ark., 2015).

Kandula ve ark. (2005) web sunucularını DDoS saldırılarına karşı korumak için istemcinin bir insan tarafından kontrol edilip edilmediğini belirlemek için grafiksel bir test olan CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) sistemini önermektedir. Kandula ve ark. tarafından önerilen grafiksel test yöntemi; WEB sitelerine karşı yapılan DDoS saldırılarının önlenmesinde güçlü bir bileşen olmuştur (Kandula ve ark., 2005).

DDOS algılama sistemleri konusunda Mirkovıc ve ark. (2005) ile Chen ve Ark. (2009) çalışmalar yapmıştır. Mirkovic ve ark. (2005) D-WARD olarak adlandırdıkları Saldırı Kaynağı-Hedef arasındaki ağlarda konuşlandırılan istatistiksel gözlem yaklaşımı ile oluşturulan DDoS savunma mimarisi tasarlamıştır. Giden trafik ve adres seti ile şebekenin geri kalan kısmı arasındaki iki yönlü trafiği izlemek amacıyla, önceden belirlenmiş bir adres seti yapılandırılmıştır. Chen ve Ark. (2009) iki örneklemeli T-testine dayanan etkili bir DDoS algılama tekniğini sunmaktadır. Bu yaklaşımda ilk olarak normal trafiğe ait SYN Varış Oranı (SAR: SYN Arrival Rate) örneklem dağılımlarını araştırılmıştır. Normal bir dağılıma uyup uymadığı kontrol edilir. DDoS saldırı trafiği ile yasal trafik arasındaki SAR sapmasını hesaplanarak SYN ve ACK paketlerinin sayıları arasındaki farkı bulunmaktadır. İki örneklemeli T-testinde; gelen trafik varış oranı ile normal trafik varış oranı arasındaki farklar karşılaştırılır. Önemli bir farklılık bulunursa, trafiğin saldırı trafiği olabileceği onaylanır. Bununla birlikte, düşük oranlı bir DDoS saldırısı olması durumunda, varış hızı testi yararlı olmayabilir ve bu nedenle, saldırı amacına ulaşabilir. Böyle bir durumda, Chen'in yöntemi, iki grubun farklı sayıda SYN ve ACK paketleri ile iki örneklemeli T-testi ile karşılaştırmasını yapılmaktadır (Mirkovic ve ark., 2005).

Jin ve ark. (2004) tarafından geliştirilen Çok Değişkenli Korelasyon Analizi (MCA: Multivariate Correlation Analysis) ağ trafiğinde ani değişimleri ölçmek için etkili bir yaklaşımdır. SYN Flooding saldırı tespit modelinde MCA sayesinde bir

ağdaki anormal trafiği basit ama etkili bir şekilde tanımlamak için kullanılabileceğini göstermektedir (Jin ve ark., 2004).

DDOS algılama sistemleri konusunda diğer bir çalışma Hwang ve ark. (2003) tarafından yapılmış olup; sunucu, yönlendirici ve ana bilgisayarları gibi ağ kaynaklarını DDoS saldırılarına karşı korumak için NetShield olarak adlandırılan verimli bir DDoS savunma çözümü sunmaktadır. NetShield IP üzerinden veri madenciliğini kullanarak DDoS saldırılarını tespit edecek şekilde tasarlanmıştır. Bu algılama yazılımı yalnızca DDoS saldırılarına karşı savunmakla kalmaz, aynı zamanda diğer zararlı ağ solucanları ve virüsleri de tespit edebilmektedir. Bu sayede saldırıların önlenmesi ve saldırı raporunun hazırlanmasını sağlamaktadır (Hwang ve ark., 2003).

Bir başka çalışmada, Jalili ve ark. (2005) istatistiksel bir ön-işlemci kullanarak, denetimsiz sinir ağı uygulayan etkili bir DDoS algılama sistemi geliştirmişlerdir. Yöntemde, sinir ağında eğitim vektörünü oluşturmada bir ön-işlemci kullanarak başlangıçta ağ trafiğinden istatistiksel bilgiler elde edilmektedir (Jalili ve ark., 2005).

Kim ve ark. (2008) birden fazla DDoS saldırı tipinin hızlı bir şekilde algılanmasını sağlamak için kural tabanlı savunma yöntemi sunmaktadırlar. Yöntemde, önce belirli bir zaman aralığı için trafik verileri toplanmakta sonrasında da bu veriler analiz edilmektedir. Yöntem, anormal trafiği tanımlamak için bir grup kurala sahiptir ve DDoS saldırı türlerini gerçek zamanlı olarak algılamak için bu kural grubunun etkili bir şekilde kullanılması amaçlanmaktadır. Bu yöntem aynı zamanda alarm sonrası teşhis ve sahte alarmları azaltmak için kritik değerleri yeniden hesaplama olanağını da sağlamaktadır (Kim ve ark., 2008).

Li ve ark. (2002) kaynak IP adres bilgilerini her bağlantıda dinamik olarak güncellemek için SAVE protokolünü geliştirmiştir. Belirli bir bağlantı için kaynak IP adresleri listesinde yer almayan IP adresleri bloke edilmektedir. SAVE, her bir Router bağlantısı için güncel bir tablo oluşturmakta ve geçerli IP adresleri hakkındaki bilgileri sık sık güncellemektedir. SAVE protokolünün giriş filtreleme sistemine kıyasla önemli bir avantajı, gelen link tablosu düzenli olarak güncellenmesidir. DDoS saldırısının sadece sahte IP adreslerinden yapılmaması durumunda SAVE'de güvenli bir yöntem olmaktan çıkmaktadır (Li ve ark., 2002).

DDoS saldırıların gerçekleştirilmesi maksadıyla saldırganlar tarafından birçok saldırı aracı geliştirilmiştir. Günümüzde internet ortamından kolayca indirebilen bu araçlara LOIC (Pras ve ark., 2010) veya HOIC gibi gelişmiş uygulamalar örnek verilebilir. Bhattacharyya ve Kalita (2016) ağ güvenlik araçları, saldırı paketlerini yakalama, ağ trafiğini izleme/analizi ve trafik davranışının görselleştirilmesi gibi birçok alanda değerlendirmelerde bulunmuştur. Giderek artan saldırı çeşitliliği ve karmaşıklığı nedeniyle özellikle saldırı araçlarının gelişimi ile saldırı amacıyla geliştirilen araçların özellikleri, yeteneklerini ve nasıl kullanıldıkları hakkında bilgiler sunmaktadır.

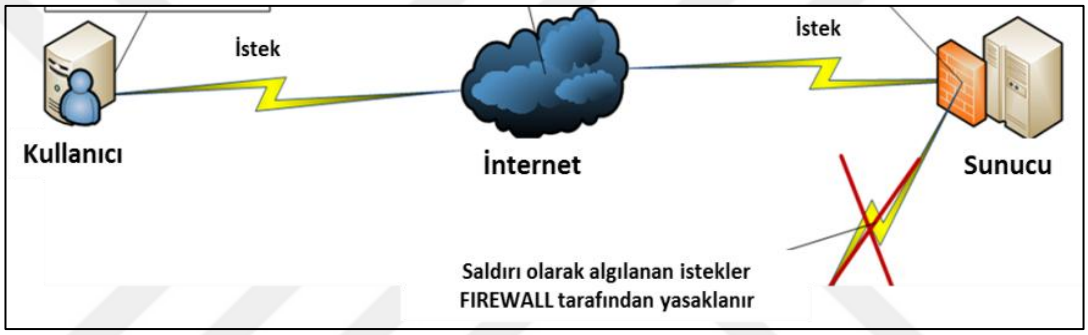
Yapılan literatür çalışması ve analizler sonucundan DDoS ve BOTNET saldırılarının önlenmesi maksadıyla geliştirilen sunucu yapıcı bu bölümde anlatılmaktadır.

4.1. Geleneksel Sunucu Mimarisi

Geleneksel sunucu mimarisinde (Şekil 4.1) web sayfası adres bilgisi ve IP adresleri DNS sunucularında bulunmaktadır. Kullanıcı tarafından yapılan istekler DNS sunucusu marifetiyle IP adresine erişim sağlanmaktadır. Gelen istek ilk önce güvenlik duvarına (FIREWALL) iletilir. Güvenlik duvarına gelen paket incelenerek

analiz edilir. Paket güvenilir bir istek içeriyorsa, paket uygulama/web sunucusuna iletilir, paket zararlı bir istek içeriyorsa engellenir.

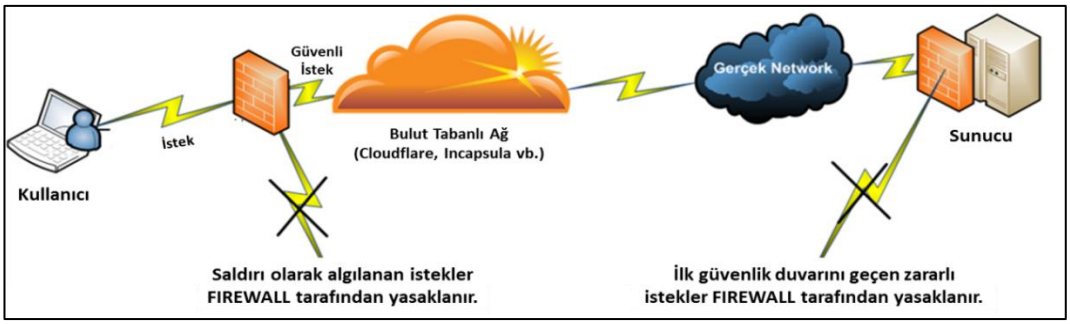
Büyük çaplı DDoS saldırısına maruz kalan FIREWALL'lar çoğu zaman bu paketleri kaçırabilmektedir. Bu durumda saldırı amacına ulaşmış olur. Bu tür sunucu yapısında saldırgan direkt olarak sunucu ile iletişim kurabilmektedir. Bu tarz bağlantılarda, güvenlik en düşük düzeydedir. DDoS saldırısı yapıldığında sunucu ile direkt iletişime geçilebildiğinden dolayı sunucu bu olaydan fiili olarak etkilenmiş olur.



Şekil 4.1. Geleneksel sunucu ağ mimarisi (Çelik, 2012)

4.2. Bulut Tabanlı Sunucu Mimarisi

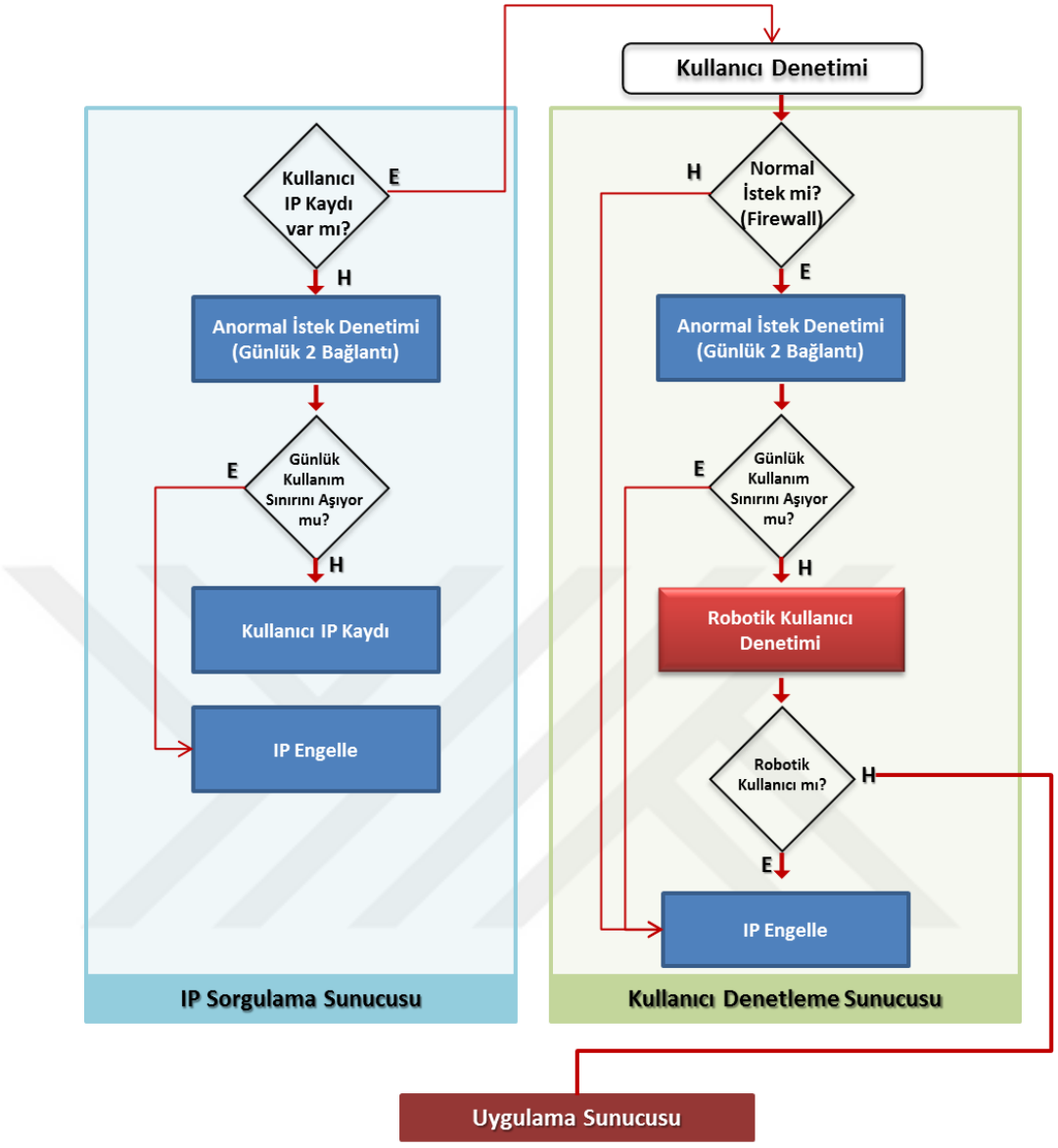
Bulut Tabanlı Sunucu mimarisinde (Şekil 4.2.), saldırganın gönderdiği tüm istekler önce Bulut Tabanlı Ağ Sunucularının ön tarafında bulunan güvenlik duvarına iletilir. Gelen bu istekler, güvenlik duvarı ile süzüldükten sonra ilgili web sunucusuna iletilir. Sunucunun vermiş olduğu cevaplar da aynı yol ile önce bulut tabanlı ağ sunucularına iletilir ve sunucularından kullanıcıya iletilir. Kullanıcı web sitesi ile fiziksel bir iletişime geçememektedir. Dolayısı ile gelecek olan tüm DDoS saldırıları bulut tabanlı ağ sunucularına iletilir. Burada yüksek bant genişliği, DDoS algılama, önleme ve IP filtreleme sistemleri ile güvenlik sağlanır.



Şekil 4.2. Bulut tabanlı sunucu ağ mimarisi (Çelik, 2012)

4.3. DoS/DDoS Saldırılarına Karşı Önerilen Kullanıcı Kayıtlı Sunucu Mimarisi

Son yıllarda yapılan DDoS saldırılarının boyutu, mevcut altyapı ve internet servis sağlayıcıların sunduğu bant genişliğinin çok üstündedir. 2016 yılında Fransız merkezli bir hosting firması olan OVH'yi hedef alan DDoS saldırı 1 Tbps gibi devasa bir trafiğe ulaşmıştır. Bu boyutlara ulaşmasını sağlayan mobil cihazlar üzerindeki zararlı yazılım ile ele geçirilen BOTNET saldırılarıdır. Böyle büyük bir saldırı karşısında kullanıcılara hizmet vermek için geliştirilen ve önerilen sunucu mimari akış şeması Şekil 4.3'de verilmektedir.



Şekil 4.3. DoS/DDoS saldırılarına karşı önerilen sunucu mimarisi

İnternet üzerinden hizmet veren birimlerin geleneksel yöntemlerin dışına çıkmadığı sürece bu tür saldırılar ile baş etmesi mevcut koşullarda imkânsızdır. Örneğin bir bankanın internet sitesine ulaşmak istediğinizde; web adresi yazılarak DNS sunucusu tarafından IP adresine yönlendirilmektedir. Bu durum DNS'de kayıtlı olan IP adresinin saldırılara açık olması anlamına gelmektedir. Bulut Tabanlı Sunucu ve önerilen sunucu mimarisinde Bankacılık Web adresi hiçbir zaman DNS sunucu kayıtlarında bulunmamaktadır. Bu yöntemde kullanıcılar Uygulama Sunucusuna direkt ulaşamamaktadır. Bulut tabanlı sunucu yapısında kullanıcıların kayıtları

istekler üzerinden tutulmaktadır. Kullanıcı davranış tabanlı filtreleme sistemi kullanılmaktadır. Bu durum bazı durumlarda normal kullanıcıların engellenmekte, bazen de saldırganların IP'lerine izin vererek saldırının başarıya ulaşmasına sebebiyet vermektedir. Çünkü kullanıcıların robotik davranışları test edilmemektedir. Bizim önerimizde kullanıcıların kayıtları manuel yapılmakta ve kullanıcının robotik olup olmadığı denetlenmektedir. Bu sayede uygulama sunucusuna erişim kontrollü olarak kısıtlanmaktadır. Bu kapsamda önerilen sunucu yapısı;

IP Sorgulama Sunucusu; sanal sunucular üzerine kurulmuş aynı işlevi gerçekleştirin birden fazla sunucudan oluşmaktadır. Saldırı Algılama Sistemi ile hizmet veren sunucunun bir saldırı karşısında devre dışı kalması durumunda, diğer sunucu aynı görevi otomatik olarak üzerine almaktadır. Sunucular farklı olsa da, kullanıcı IP kayıtları aynı veritabanı sunucusunda tutulmaktadır. Bu sunucunun en önemli işlevi saldırı anında yeni kullanıcı kaydı almamasıdır.

Kullanıcı Denetleme Sunucusu; IP adresi kaydı olan kullanıcıların virüs bulaşması sonucu istemsiz isteklerde bulunup bulunmadığını denetlemek için Robotik Kullanıcı Denetimi yapılmaktadır. Bu maksatla kullanılan yöntem, Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA)'dir. Hizmet almak isteyen kullanıcının yapmış olduğu isteklerin; robotik davranış sergilemediği, insan tarafından kullanıldığını ispatlaması gerekmektedir. Bu bölümü geçemeyen kullanıcı IP adresi engellenerek istek yapması kısıtlanmaktadır.

Uygulama Sunucusu, IP kaydını yapmış ve Kullanıcı Denetleme Sunucusundan başarı ile geçen kullanıcılar bu sunucudan istemiş olduğu hizmeti endirekt olarak alabilmektedir Bu yöntem ile uygulama sunucusu IP adresi DNS sunucusu ile paylaşılmamakta, DDoS maksadıyla saldırıya uğraması engellenmektedir.

5. SONUÇ VE ÖNERİLER

Bu çalışmada DDoS saldırılarını algılama, önleme ve saldırı maksadıyla kullanılan araçlara ilişkin mevcut en son teknolojik araştırmalar hakkında ayrıntılı bilgiler verilmiştir. Ayrıca BOTNET teknolojisinin yapısı ve mimarisi ile mobil cihazlar üzerinden DDoS saldırıların nasıl yapıldığı örnekleriyle anlatılmıştır. Bu kapsamda; saldırganların DDoS saldırılarını nasıl planladığı, TCP/IP ve OSI referans model katmanlarının hangi katmanında hangi tür DDoS saldırıların nasıl yapıldığı konusu incelenmiş.

DDoS saldırılarını tespiti için çözüm etkinliğini değerlendirmek uygun bir önlem geliştirmek için mutlak bir zorunluluktur. Geliştirilen önlem; sistemin tarafsız bir şekilde değerlendirilmesi için doğruluk, güvenilirlik, uyumluluk, ölçeklenebilirlik, zamanlama ve tutarlılık gibi savunma sisteminin olası tüm yönlerini dikkate alınmalıdır. Son yıllarda gerçekleştirilen saldırı türleri ve yoğunluklarına ait istatistiki bilgilerin analizi sonucunda karşılaşılan zorluklar aşağıda sunulmuştur:

a. Sahte IP'ler DDoS saldırganları tarafından yaygın olarak kullanılan etkili bir tekniktir. Birçok araştırmacı, sahte IP kullanımının BOTNET tabanlı DDoS saldırıları bağlamında ilişkilendirmesini düşük seviyede tutsa da, saldırganlar tarafından bu yöntemin ucuz ve etkili olması nedeniyle kullanılmasına devam edilmektedir. Sahte IP adres trafiğinin filtrelenmesi için giriş-çıkış filtreleri çok etkili olarak kabul edilse de, saldırganların sahte IP şemalarını kullanması ile bu tür koruma yöntemlerini atlatabildikleri değerlendirilmektedir. Bu nedenle kaynak IP sahtekârlıklarına karşı çözümlerin geliştirilmesi hala önemli bir araştırma konusu olmaya devam etmektedir.

b. UDP Flooding saldırıları araçlarında paket boyutunun rastgele seçilmesi, kaynak IP sahtekârlığı ve diğer üstbilgi alanlarının rastgele kullanılmasıyla saldırı trafiği üretilebilir. Mevcut saldırı araçlarının hiçbiri tüm bu özelliklerin birleşimi ile tasarlanmamıştır. Dolayısıyla yeni nesil saldırıların tüm bu özellikleri birleştirecek şekilde saldırı araçlarının geliştirilmesi muhtemel olduğu ve çeşitli protokollerde çalışan Flooding saldırılarının oluşturulabileceği düşünülmelidir. Ağ geliştiricilerinin özellik bu tür kombinasyonu saptamak için yöntemler geliştirmesine ihtiyaç vardır.

c. Çoğu DDoS algılama ve önleme yönteminin birden çok kullanıcı parametresine bağlı olması ve yöntem performansının bu parametre değerlerine oldukça duyarlı olması gözarda edilmez bir gerçektir. Gelecekte yapılacak çalışmalarda bu parametre değerlerini daha doğru tahmin edebilen sezgisel yöntemler geliştirilmedir.

c. DDoS saldırı anomalilerini gerçek zamanlı olarak hizmet kalitesinden ödün vermeksizin bir savunma sisteminin tasarlanması oldukça zor bir iştir. Meşru kullanıcılara verilen hizmet kalitesinden ödün vermeden yüksek ve düşük hızlardaki DDoS saldırılarını gerçek zamanlı olarak izleyen ve algılayan entegre bir savunma sisteminin geliştirilmesine ihtiyaç vardır.

Diğer bir husus ise araştırmacılar tarafından DDoS saldırılarını tespit etmek, önlemek ve etkisini azaltmak için çeşitli yenilikçi ve pratik çözümler sunmuş olsa da, son yıllarda sofistike saldırı tehditlerinin geliştirilmesinde mobil cihazların kullanılması saldırı etkisini arttırmıştır. Akıllı Mobil cihazların kullanım oranın artması zararlı yazılım geliştiricilerin bu alana olan ilgisini arttırmıştır. Büyük bir kullanım alanına sahip olan bu cihazlar güvenlik açısından gelişme döneminde olan mobil işletim sistemleri nedeniyle zararlı yazılım geliştiricilerin hedefi haline gelmiştir. Bu tür cihazlarda hassas veriler, iletişim bilgileri, şifreler ve kredi kartı

numaraları dahi bulunmaktadır. Neredeyse her gün yeni bir mobil zararlı yazılımı ortaya çıktığı görülmektedir. Mobil BOTNET'ler ile ilgili elde edilen bulgular şunlardır;

- Yapılan analizde BOTNET temel özelliklerinin DDoS saldırıları amacıyla geliştirildiği,
- ANDROID işletim sisteminde güvenlik açıklıkların zararlı yazılım geliştiricileri tarafından büyük oranda kullanıldığı,
- Üst düzey yetenekler ve teknolojilere sahip olan telefonların güvenlik konusunda yeterli seviyede olmadığı ve sürekli yanımızdan ayırmadığımız bir casusa dönüşebildiği,
- Mobil BOTNET'lerin 2015 yılından itibaren artarak DDoS saldırılarında kullanıldığı, hatta ana omurgasını oluşturduğu,
- IoT, akıllı mobil cihazlar, IP kamera ve internete bağlı cihazlara ait güvenlik güncellemelerinin yeterli olmadığı,
- BOTNET temel özelliklerinin; Mobil BOTNET Geliştirme Modeli bütün aşamalarında ortaya çıktığı,
- Mobil cihaz kullanıcıların BOTNET ve DDoS saldırıları konusundaki farkındalığın yeterli seviyede olmadığı ve yapılan bu çalışmanın bu farkındalığı artıracağı değerlendirilmektedir.

Hedefli ve koordine bir şekilde gerçekleştirilen ve mobil cihazlarla desteklenen DDoS atakları geleneksel savunma metotlarının gücünü zayıflatmaktadır. BOTNET ile DDoS saldırılarının nasıl yapıldığı konusu ele alınmıştır. Bu kapsamda, BOTNET saldırılarının DDoS amaçlı olarak kullanımı araştırılmış, BOTNET saldırılarının ortak özellikleri belirlenmiş, bu özelliklerle BOTNET modelleme adımları arasındaki ilişki saptanmış, uygulamalarda söz konusu özelliklerin bulunup bulunmamasını tespit yöntemleri ve BOTNET ve DDoS saldırılarına karşı korunmak için Kullanıcı Kayıtlı Sunucu mimarisi önerilmiştir.

ÖZET

Dağıtık Servis Dışı Bırakma Saldırılarının İncelenmesi ve Korunma Yöntemleri

Bilişim alanında en çok görülen siber saldırıların başında Servis Dışı Bırakma (DoS - Denial of Service) ve Dağıtık Servis Dışı Bırakma (DDoS - Distributed Denial of Service) saldırıları gelmektedir. DoS saldırısı; 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 "dağıtılmış" (distributed) olarak gerçekleştirildiğinde DDoS saldırısı olarak adlandırılmaktadır. DDoS saldırıları için ele geçirilmiş köle olarak adlandırılan bilgisayarlar kullanılmaktadır. Bu saldırıların amacı, normal kullanıcılar için sunucu hizmetini kısmen veya tamamen kullanım dışı bırakmaktır. En temel çözüm olarak, İnternet Servis Sağlayıcı (İSS) (ISP - Internet Service Provider) bant genişliğinin artırılması veya farklı bir İSS'dan hizmet alınmasıdır. Ayrıca yeni geliştirilen istatiksel yöntemler ile kullanıcı filtreleri uygulanmaktadır. Bu filtreler; mevcut kullanıcılarla, saldırı amacıyla kullanılan bilgisayarları ayırt etmek için istatiksel yöntemler ve kullanıcı davranış modelini uygulamaktadır. Kullanıcı davranış modelinde, toplanan veriler belirli matematiksel işlemlerle; saldırgan IP'lerinin engellenmesi amaçlanmaktadır. Bu yöntemin en büyük dezavantajı, saldırı yapmayan sadece hizmet almaya çalışan normal kullanıcıların da engellenmesidir. Bu tez çalışmasında; son yıllarda gerçekleşen çeşitli DoS/DDoS saldırıları analiz edilmiş, algılama ve önleme teknikleri incelenmiş, kullanılan araçlar araştırılmış ve DDoS saldırıları engelleme maksadıyla sunucu mimarisi önerilmiştir.

Anahtar Kelimeler: Ağ, Dağıtık Servis Dışı Bırakma, Köle Bilgisayar, Siber Saldırı, Sunucu

SUMMARY

A Survey to Detection and Protection Methods of Distributed Denial of Service Attacks

Denial of Service (DDoS) and Distributed Denial of Service (DDoS) attacks are among the most common cyber-attacks. DoS attacks intent to prevent a certain server providing its service to the users in other words. It disables the server without the need to temper the information system. When a DoS attack is performed "simultaneously" over multiple computers, it becomes a disturbed DoS(DDoS) attack. Computers used for DDoS attacks are called slaves. Main purpose of a DDoS attacks is to partially or completely disable the server or some of its services. Basic solution to prevent a DDoS attack is to increase the bandwidth of the server provided by Internet Service Provider (ISP) or to get internet service from different ISPs. In addition, user filters created with newly developed statistical methods are also used to prevent DoS attacks. These filters apply statistical methods and user behavioral models to distinguish regular users from attacking computers. In user behavior model collected data are analyzed by specific mathematical operations and applied to prevent attacking IPs. Main disadvantage of this method is in some cases, that non-attacking regular users who are just trying to reach a service may also be blocked. In this thesis study; various DoS/DDoS attacks which occurred in recent years have been analyzed, detection, prevention techniques and tools were examined. Based on these studies a server architecture has been created and proposed to prevent DDoS attacks.

Keywords: Cyber Attack, Distributed Denial of Service, Network, Server, Slave Computer.

KAYNAKLAR

ANDROID (2017). Manifest permission list, Erişim Adresi: [https://developer.ANDROID. com /reference/ANDROID/Manifest.permission.html] Erişim Tarihi: 22/03/2017

ANTONIOU S (2009).The ping of death and other DOS network attacks.

ARBOR (2017). *Arbor Networks Special Report 2017*, **12**, 34.

ARSTECHNICA (2017). 10 million android phones infected by all-powerful auto-rooting apps, Erişim Adresi: [https://arstechnica.com/security/2016/07/virulent-auto-rooting-malware-takes-control-of-10-million-ANDROID-devices/], Erişim Tarihi:27/02/2017.

ATZORI L, IERA A, MORABITO G (2010). The Internet of things: A survey. *Computer Networks 54*, 2010, 2787-2805.

AU KWY, ZHOU Y, HUANG Z, GILL P, LIE D (2011). Short paper: a look at smartphone permission models, 1st ACM workshop on Security and privacy in smartphones and mobile devices, *CCS 2011*, 63–68.

BAILEY M, COOKE E, JAHANIAN F, YUNJING X, KARIR M (2009). A survey of BOTNET technology and defenses, *Cybersecurity Applications & Technology Conference for Homeland Security CATCH 2009*, 299-304.

BHATTACHARYYA D K, KALITA J K (2013). *Network Anomaly Detection: A Machine Learning Perspective*, CRC Press, USA.

BHATTACHARYYA DK, KALITA J K(2016). *DDOS Attacks Evolution, Detection, Prevention, Reaction and Tolerance*, 98-196.

BİLGEM (2015). *DDoS ile Mücadele Kılavuzu*.

BRENNER, S W, GOODMAN M D (2002). In defense of cyberterrorism: an argument for anticipating cyber-attacks, *University of Illinois Journal of Law, Technology & Policy*.

BRISCOE N (2000). Understanding the OSI 7-layer model, *PC network advisor*, **120**, 13.

BTRISK (2017). Android Uygulamalara Malware Yerleştirme, Erişim Adresi: [http://blog. btrisk.com/2015/08/android-uygulamalara-malware-yerlestirme-1.html] Erişim Tarihi: 22/02/2017.

CASTILLO CA (2016), ANDROID malware past, present, and future (McAfee), Erişim Adresi: [https://pdfs.semanticscholar.org/5735/6502310474ba9564ec8f581494b8de50 b3e5.pdf], Erişim Tarihi: 22/02/2016.

CHECKPOINT(2017). A whale of a tale: humming bad returns 2017, Erişim Adresi: [http://blog.checkpoint.com/2017/01/23/hummingbad-returns/] Erişim Tarihi: 27/02/2017.

CHEN T, REN J (2009). Bagging for gaussian process regression. *Neurocomputing*, 7**2**, 1605-1610.

ÇELİK E (2012). Web sunucularında DDOS-BOTNET saldırılarını minimize etme, Erişim Adresi:[http://www.mshowto.org/web-sunucularinda-DDOS-botnet-saldirilarini-minimize-etme-DDOS-ataklar-nasil-onlenir.html], Erişim Tarihi: 22.02.2017

ÇELİKBİLEK İ (2016). TCP SYN saldırısının etkilerini azaltmak için yeni SYN çerezleri gerçeklemesi, 2-3.

CRAIG AS, CHILLER J, HARLEY D (2007). *BOTNETs the Killer Web App*, Syngress, 13.

DESAI N (2009). Intrusion prevention systems: The next step in the evolution of IDS, 1-12.

DOULIGERIS C, MITROKOTSA A (2003). DDOS attacks and defense mechanisms: classification and state-of-the-art, *Computer Networks*, **44**, 643-666.

ENCK W, ONGTANG M, MCDANIEL P (2009). On lightweight mobile phone application certification, *16th ACM Conference on Computer and Communication Security*, New York, 235-245.

ESLAHI M, SALLEH R, ANUAR N B (2012). A new generation of BOTNETs on mobile devices and networks, *International Symposium On Computer Applications And Industrial Electronics*, 262-266.

FELT A. P, GREENWOOD K, WAGNER D (2012). The effectiveness of application permissions, *2nd Usenix Conference ON Web Application Development*, 75-86.

FERGUSON P, SENIE D (2000). Network ingress filtering: defeating denial of service attack which employ IP source address filtering, *Internet Engineering Task Force*.

FLO A, JOSANG A (2009). Consequences of BOTNETs spreading to mobile devices, Proc. *14th Nordic Conference on Secure IT Systems*, 37-43.

GARBER L(2000). Denial-of-service attacks rip the internet. *IEEE Computer*, **33**, 12-17.

GORLA A, TAVECCHIA I, GROSS F, ZELLER A (2014). Checking app behavior against app descriptions, *36th International Conference on Software Engineering*, 1025-1035.

GÜRKAYNAK M (2011). Reel dünyada sanal açmaz: Siber alanda uluslararası ilişkiler, *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, **16**, 2, 264.

HACHEM N, MUSTAPHA Y, GRANADILLO G, DEBAR H (2011). BOTNETs: lifecycle and taxonomy, *Network and Information Systems Security*, 1-8.

HOLL P (2015). Exploring DDoS defense mechanisms, *Network Architectures and Services*, 25-32.

HOQUE N, BHUYAN M H, BAISHYA R, BHATTACHARYYA D, KALITA J (2013). Network attacks: taxonomy, tools and systems, *Journal of Network and Computer Applications*, **40**, 307-324.

HWANG K, DAVE P, TANACHAIWIWAT S (2003). Netshield: Protocol anomaly detection with data mining against DDoS attacks, *6th Int'nl Symposium on Recent Advances in Intrusion Detection*, 8-10.

IoT (2017). IoT Powered DDoS attacks and SCADA incidents will make top security headlines in 2017, Erişim Adresi: [https://businessinsights.bitdefender.com/iot-ddos-attacks-scada-incidents] Erişim Tarihi: 22/03/2017.

JAESEO L, HYUNCHEOL J, JUN-HYUNG P, MINSOO K, BONG-NAM N (2008), The Activity Analysis of Malicious HTTP-Based BOTNETs Using Degree of Periodic Repeatability, *International Conference on Security Technology*, 83-86.

JALILI R, IMANI-MEHR F, AMINI M, SHAHRIARI H R (2005). Detection of distributed denial of service attacks using statistical preprocessor and unsupervised neural networks, *International Conference on Information Security Practice and Experience*, 192-203.

JIN S, YEUNG DS (2004). A covariance analysis model for DDoS attack detection. In Communications, *IEEE Communications Society*, 1882-1886.

JOSHI S, KHANNA R, JOSHI L. K (2015). ANDROID BOTNET: An upcoming challenge, *IOSR Journal of Computer Engineering*, 5-10.

KANDULA S, KATABI D, JACOB M, BERGER A (2005). BOTs-4-sale: Surviving organized DDoS attacks that mimic flash crowds, *2nd Conference on Symposium on Networked Systems Design & Implementation*, 287-300.

KANG M S, LEE S B, GLIGOR V D (2013). The crossfire attack, *IEEE*, 127-141.

KAPLAN Y (2000). *Veri Haberleşmesi Temelleri*, İstanbul.

KHALO A (2016). A guide to understanding android app permissions & how to manage them, Erişim Adresi: [http://www.hongkiat.com/blog/ANDROID-app-permissions/] Erişim Tarihi: 28/09/2016.

KILINÇ D, BOZYİĞİT F, BORANDAĞ E, YÜCALAR F (2016). Sınıflandırma tabanlı zombi bilgisayar tespit sistemi, *Akademik Bilişim 2016*, 1-5.

KIM S, KIM B, LEE J, HWANG C (2008). Rule-based defense mechanism against DDoS attacks. *In Proceedings of the World Congress on Engineering*, **1**, 1-6.

KOÇASLAN MD (2015). DDOS saldırıları ve korunma yöntemleri üzerine simülasyon uygulamaları, *Beykent Üniversitesi Fen Bilimleri Enstitüsü YL Tezi*, 5.

KUMAR PAR, SELVAKUMAR S (2013). Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems. *Computer Communications*, **36**, 303-319.

LI J, MIRKOVIC J, WANG M, REITHER P, ZHANG L (2002). SAVE: Source Address Validity Enforcement Protocol, *IEEE INFOCOM*, 1557-1566.

MANJUNATH V (2011). Reverse engineering of malware on ANDROID, *MSc Computer Security University of ESSEX*.

MINCH RP (2004). Privacy issues in location-aware mobile devices, 37th Annual Hawaii International Conference, *IEEE Computer Society*, 50.

MIRKOVIC J, DIETRICH S, DITTRICH D, REIHER P (2005a). *Internet Denial of Service: Attack and Defense Mechanisms*, Prentice Hall.

MIRKOVIC J, REIHER P (2004). A taxonomy of DDOS attack and DDOS defense mechanisms. *SIGCOMM Computer Communication Review*, 39-53.

MIRKOVIC J, REIHER P (2005b). D-WARD: A source-end defense against flooding denial-of-service attacks, *IEEE Transactions Dependable and Secure Computing*, **2**, 216-232.

NAZRUL H, DHRUBA K, B, KALITA J K (2015). BOTNET in DDoS attacks: Trends and challenges", *IEEE Communication Surveys & Tutorials*, **17**, 2242-2270.

NTV (2017). Türkiye genelinde elektrik kesintisi, Erişim Adresi: [http://www.ntv.com.tr/turkiye/elektrik-neden-kesildi-turkiye-genelindeelektrik-kesintisi, RhfwqMiNNkOUj5_sO12qJg] Erişim Tarihi: 22/03/2017.

PARK K, LEE H (2001). On the effectiveness of route-based packet filtering for distributed dos attack prevention in power law internets. SIGCOMM computer communication review , 31,15-26.

PIETERSE H, OLIVIER M S (2012), Android BOTNETs on the rise: Trends and characteristics, *IEEE ISSA*, 1-5.

PRAS A, SPEROTTO A, HOFSTEDE R (2010). Attacks by "Anonymous" WikiLeaks Proponents not Anonymous, *CTIT Technical Report 10.41*, 1-10.

SINGER PW (2014). *Cybersecurity and Cyberwar*, 15.

SPREITZENBARTH (2017). Forensics blog, Erişim Adresi: [http://forensics.Spreitzenbarth.de/ANDROID-malware/], Erişim Tarihi: 22/02/2017.

STM (2017). Siber tehdit durum raporu ekim-aralık 2016, Erişim Adresi: [https://www.stm.com.tr/documents/file/Pdf/Siber Tehdit Durum Raporu Ekim-Aralık 2016.pdf] Erişim Tarihi: 22/04/2017.

TAO P, LECKIE C, KOTAGIRI R (2007). Survey of network-based defense mechanisms countering the DoS and DDoS problems, *ACM Computing Surveys*, **39**, 1-42.

TECHWORLD (2017). Eurograbber SMS trojan steals €36 million from online banks, Erişim Adresi: [http://www.techworld.com/news/security/eurograbber-sms-trojan-steals-36-million -from-online-banks-3415014/] Erişim Tarihi: 22/03/2017.

THAKKAR NB (2015). An analytical model based on permissions for detecting malware for an innovative platform android: Mobile operating system, *KAAV International Journal of Science, Engineering & Technology*, **2**, 23.

THOTTAN M, LIU G, JI C (2010). Anomaly detection approaches for communication networks, *Computer Communications and Networks*, 239-261.

TODD M G (2009). Armed attack in cyberspace: deterring asymmetric warfare with an asymmetric definition, *Air Force Law Review*, **64**, 68-69.

UDP (2017). Understanding UDP flood attacks, Erişim Adresi: [https://www.juniper.net/documentation/en_US/junos/topics/concept/denial-of-service-network-udp-flood-attack-understanding.html] Erişim Tarihi: 22/04/2017.

USA DEPARTMENT OF DEFENCE (2017). *Department Of Defence Dictionary Of Associated Terms*, 61.

WIKIPEDIA (2017). Denial of service attack, Erişim Adresi: [https://tr.wikipedia.org/wiki/Denial-of-service_attack] Erişim Tarihi: 22/03/2017.

WELIVESECURITY (2017). Released ANDROID malware source code used to run a banking BOTNET, Erişim Adresi: [http://www.welivesecurity.com/2017/02/23/released-ANDROID-malware-source-code-used-run-banking-BOTNET/] Erişim Tarihi: 22/03/2017.

XIANG Y, ZHOU W, CHOWDHURY M(2010). *A Survey of Active and Passive Defence Mechanisms against DDoS Attacks*, Deakin University, 1-42.

XIE Y, YU S (2009). Monitoring the application-layer DDoS attacks for popular websites. IEEE/ACM Transactions on Networking 17, 15-25.

YATAGAI T, ISOHARA T, SASASE I (2007). Detection of HTTP-get flood attack based on analysis of page access behavior, IEEE, 232-235.

YU S, ZHOU W, DOSS R, JIA W (2011). Traceback of DDoS attacks using entropy variations, *IEEE Transactions on Parallel and Distributed Systems*, **22**, 412-425.

ZENG Y (2012). On detection of current and next-generation BOTNETs, *Ph.D. Thesis*, , Computer Science and Engineering, University of Michigan.

ZENG Y, SHIN K G, HU X (2012). Design of SMS commanded-and-controlled and P2P-structured mobile BOTNETS. *ACM Conference on Security and Privacy in Wireless and Mobile Networks WISEC 2012*, 137-148.

ZHOU W, ZHOU Y, JIANG X, NING P (2012). Detecting repackaged smartphone applications in third-party ANDROID marketplaces, *ACM Conference on Data Application Security and Privacy*, 317-326.

ÖZGEÇMİŞ

I- Bireysel Bilgiler

Adı : Ersin

Soyadı : MASUM

Doğum Yeri ve Tarihi: Erzurum, 1977

Uyruğu : Türkiye Cumhuriyeti

Medeni durumu : Evli

E-Posta : ersinmasum@gmail.com

II- Eğitimi

2015 - 2017 : Ankara Üniversitesi Adli Bilimler Enstitüsü Adli Bilişim A.D

1995 - 1999 : Kara Harp Okulu Sistem Mühendisliği

1991- 1995 : Işıklar Askeri Lisesi

Yabancı Dil : İngilizce