Mobil BOTNET ile DDoS Saldırısı

Ersin MASUM[1], Refik SAMET[2]

[1]Sağlık Bilimleri Enstitüsü Disiplinlerarası Adli Bilimler (Adli Bilişim) A.B.D., Ankara Üniversitesi, Ankara, Türkiye
[2]Bilgisayar Mühendisliği, Mühendislik Fakültesi, Ankara Üniversitesi, Ankara, Türkiye
ersinmasum@gmail.com, samet@eng.ankara.edu.tr
(Geliş/Received: 17.04.2017; Kabul/Accepted: 07.04.2018)
DOI: 10.17671/gazibtd.306612

Özet— Akıllı mobil cihazlar dünyadaki milyarlarca insanın kullandığı bir teknolojidir. Bu mobil cihazların internet, konum belirleme sistemleri (GPS), kablosuz iletişim ve sağlık uygulamaları gibi ileri düzey yetenek ve teknolojilerinin gelişimiyle kullanım oranları artmıştır. Mobil cihazların kullanım oranın artması 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 zararlı yazılımların hedefi haline gelmiştir. Buna rağmen bilgisayar ile karşılaştırıldığında daha düşük güvenlik politikalarına sahip olduğu görülmektedir. Mobil cihaz kullanıcılarının, bilgisayar kullanıcılarına nazaran güvenlik güncelleme ve uygulamalarına yeterince önem vermedikleri tespit edilmiştir. ANDROID ve iOS sektördeki en popüler mobil işletim sistemleridir. ANDROID, akıllı cihaz pazar payının büyük bir kısmına sahip olması ve açık kod kaynaklı olması nedeniyle zararlı yazılım geliştiricilerin hedefi olmaya devam etmektedir. Son zamanlarda ortaya çıkan ve ANDROID cihazlarını hedef alan en tehlikeli tehditlerden birisi BOTNET saldırısıdır. Bu makalede, mobil BOTNET saldırılarının tanımı ve hâlihazırda mevcut BOTNET ailelerinin bir analizi ve DDoS maksadıyla kullanımı örnekler ile sunulmaktadır. Bu örnekleri analiz ederek, BOTNET saldırılarının ortak özellikleri ve davranışları açığa çıkarılacaktır. Bu sayede, kullanıcı farkındalığının artması ve cihazları üzerinde gerekli güvenlik güncellemelerini yapmaları ve resmi olmayan uygulama mağazalarından elde edilmiş yazılımları daha dikkatli kullanması sağlanacaktır.

Anahtar Kelimeler— Akıllı Cihaz, Mobil İşletim Sistemi, ANDROID, Uygulama, Zararlı Yazılım, DDoS, BOTNET

DDoS Attack with Mobile BOTNET

Abstract— Smart mobile devices are used by billions of people around the world. Utilization rates of these devices have increased with the development of advanced capabilities and technologies such as the internet, global location system (GPS), wireless communications and various health applications. Increased use of mobile devices has boosted the interest of malware developers in this area as well. These devices, which have a wide spectrum of applications in various fields, have become the target of malicious software due to underdevelopment of the security aspects of mobile operating systems. They have less security policies, compared to computers. It is also revealed that mobile users, with respect to computer users, do not pay much attention to security updates and security-applications. ANDROID and iOS are the most popular mobile operating systems in mobile industry. ANDROID continues to be the target of malware developers since it is open-source and holds the bigger share of the smart device OS market. One of the most recent and dangerous threats to ANDROID devices is the BOTNET attack. In this article, the definition of mobile BOTNET attacks, an analysis of the existing BOTNET families and their utilization for DDoS attacks are presented with examples. By analyzing these examples, common attributes and behaviors of BOTNET attacks will be revealed. This will increase the awareness of users, ensure that they apply necessary security updates on their devices and use the application software retrieved from unofficial application stores more carefully.

Keywords— Smart Device, Mobile Operating System, ANDROID, Application, Malware, DDoS, BOTNET

1. GİRİŞ (INTRODUCTION)

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 ve enerjiye kadar değişen birçok sektörde 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 etkileşim halindedirler. Farklı bir anlamda 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 [1]. Siber uzay, bireylerin ve toplumların günlük yaşamlarında çok önemli faydalar ve kolaylıklar sağlamaya başlamış olsa da zararlı ve bilinçsiz kullanımdan dolayı bazı dezavantajları beraberinde bulundurmaktadır [2]. 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 içinde bazı tanımlar yapılmıştır. ABD Savunma Bakanlığı siber savaşı, "saldırıyı düzenleyenlerin temel amaçlarına ulaşmak için sahip oldukları siber kapasitenin siber alanda kullanılması" olarak tanımlamıştır [3]. 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 etkili 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 [4].

Siber alanda gerçekleşen saldırıların ve savaşların kendine özgü silahları bulunmaktadır. Bu silahlar doğrudan fiziki dünyayı hedef almasa da sanal dünya ile bütünleşmiş günlük hayatta olumsuz sonuçlara yol açabilmektedir. 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 [5].

Siber silahları iki başlıkta toplamak mümkündür. Bu silahlar genel olarak sözdizimsel (Syntactic) ve anlamsal (Semantic) tipteki silahlar olarak adlandırılmaktadır [6]. Sözdizimsel silahlar 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 bilgisayar kullanırken 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 [7]. 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 [8]. Büyük bir kullanım yelpazesine sahip olması, kullanım oranın artması ve güvenlik açısından henüz gelişme döneminde olması sebebiyle mobil işletim sistemlerine sahip cihazlar zararlı yazılım geliştiricilerin hedefi haline gelmiştir. Ayrıca mobil cihazlar bilgisayar ile karşılaştırıldığında daha düşük güvenlik politikalarına sahiptir. ANDROID ve iOS işletim sisteminin geliştirilmesiyle kullanılmaya başlanan akıllı mobil cihazlar ve akıllı olmayan cihazların bu saldırılarda kullanılması saldırının boyutunun karşı konulmaz büyüklüğe ulaşmasını sağlamaktadır.

Bilgi güvenliği; bilgilerin izinsiz erişimi, kullanımı, ifşa edilmesi, yok edilmesi, değiştirilmesi veya hasar verilmesini engellemektir. Mahremiyet, bütünlük ve bilgi ulaşılabilirliğinin korunması ortak hedeftir. Bilgi güvenliği temel fonksiyonları aşağıdaki şekilde sıralanabilir [9].

- 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 bilgi güvenliği unsurlarından sürekliliği hedef almaktadır. Süreklilik; bilginin her an ulaşılabilir ve kullanılabilir olmasını amaçlayan prensiptir. Bilişim sistemleri, kurum içinden ve dışından gelebilecek tehditlere karşı korumayı süreklilik sayesinde sağlamaktadır.

Bu makalede, mobil BOTNET saldırılarının tanımı ve hâlihazırda mevcut BOTNET ailelerinin bir analizi ve DDoS maksadıyla kullanımı örnekler ile sunulmaktadır. Bu kapsamda, BOTNET saldırılarının DDoS amaçlı olarak kullanımı araştırılmış, BOTNET saldırılarının ortak özellikleri belirlenmiş, bu özelliklerle BOTNET modelleme adımları arasındaki ilişki saptanmış, mobil uygulamalarda söz konusu özelliklerin olup olmadığının tespit yöntemleri geliştirilmiştir. Bu sayede kullanıcı farkındalığının arttırılması ve cihazları üzerinde gerekli güvenlik güncellemelerini ve resmi olmayan uygulama mağazalarından elde edilmiş yazılımları daha dikkatli kullanması sağlanacaktır.

Bu kapsamda; makalenin ikinci bölümünde ilgili çalışmalar hakkında bilgi verilmekte, üçüncü bölümde konu hakkında yapılan tespitler ortaya konulmakta ve dördüncü bölümde analiz yapılarak çözüm yaklaşımına yönelik yöntemler belirlenmektedir. Son olarak, beşinci bölümde sonuçlar sunulmaktadır.

2. İLGİLİ ÇALIŞMALAR (RELATED WORKS)

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. Nerdeyse modern yaşamının her anında var olan bu cihazlar; bazen bir hayatı kurtarırken, bazen de insanoğlunun yanından ayıramadığı bir casusa dönüşmektedir. Bu nedenle mobil cihaz güvenliği; internet, kamer, GPS ve birçok sensör ile güçlendirilen akıllı mobil telefonlar için geliştirilmesi gereken önemli bir husustur [10]. Mobil cihazlar; sağladığı kullanım kolaylığına rağmen sınırlı pil, depolama ve işlemci kısıtlamaları nedeniyle bilgisayarlara nazaran daha küçük işletim sistemleri ile çalıştırılması zorunluluktur. Bu cihazlarda kullanılan en yaygın işletim sistemi ANDROID ve iOS işletim sistemleridir. İlk olarak 2008 yılında kullanıcılara sunulan ANDROID işletim istemi, 2016 yılında cep telefonu pazarının yüzde 84,7'sine hâkim olarak en popüler mobil işletim sistemi haline gelmiştir [11]. Özellikle ANDROID işletim sistemi kullanıcılarının resmi olmayan uygulama mağazaları, forum siteleri ve hafıza kartından uygulama yükleme yetkisine sahip olması cep telefonlarına zararlı yazılım bulaşmasına imkân vermektedir. Örneğin, kullanıcı tarafından sadece hava durumu bilgisini öğrenmek için yüklenen basit bir uygulama, telefonundaki birçok yetkiye (kamera, GPS, mikrofon, rehber, hafıza erişimi vb.) sahip olabilmektedir. Bu uygulama yetkilerinin kullanıcılar tarafından düzenlenmesi ANDROID 6.0 Marshmallow sürümü ve sonrası sürümlerinde geliştirilmiştir. Daha önceki sürümlerde bu uygulama izinlerini kısıtlama yetkisi kullanıcı tarafından yapılamamaktadır. Basit bir uygulamanın kamera, konum bilgisi, mikrofon, hafıza kartı ve diğer birçok sensöre kolay bir şekilde ulaşabilmesi büyük bir güvenlik açığıdır.

Cep telefonların tehdit altında olmasındaki diğer bir sebep ise internete bağlanabilme özelliğidir. Birçok farklı cihazın aynı ortamda kullanımı sonucunda virüs, internet solucanı ve truva atları ile gerçekleştirilen BOTNET saldırıların kullanıcı için çok tehlikeli hale dönüşebilmektedir [12]. "Robot" sözcüğü ile anlamlandırılan “BOT”, belirli bir görevi bir insandan daha hızlı gerçekleştiren ve tekrar eden bir uygulamadır. “BOTNET” ise, ağ yardımıyla birbirine bağlı birkaç BOT’un bir arada kullanılmasıdır. BOTNET saldırısının üç temel unsuru; BOT, Komuta ve Kontrol (C&C) Sunucusu ve BOTMASTER’dır. BOTNET'ler yöneticisine mobil cihaza ve içeriklerine tam erişim ve denetim yetkisi sağlar. Ele geçirilen mobil cihazda ROOT izinleri sayesinde; eposta, kısa mesaj, telefon görüşme kayıtları, rehber ve video-fotoğraf gibi birçok kişisel veriye ulaşılmaktadır. Çoğu zaman kullanıcının haberi dahi olmadan BOTNET ile diğer cihazlara gizlice mesaj veya e-posta gönderilebilmektedir. Bu nedenle, mobil ağ güvenliği alanında BOTNET saldırılarının tespit edilmesi güçtür.

Bu kapsamda yapılan çalışmalarda; zararlı yazılım özellikleri ve uygulama izinleri Joshi ve ark. [13] ile Gorla ve ark. [14] tarafından incelenmiştir. Joshi ve ark. [13] zararlı yazılım özellikleri ve uygulama izinlerinin incelenmesi üzerinde yöntemler geliştirmiştir. BOTNET saldırıları arasındaki ortak özelliklerini belirlemek için izin tabanlı filtreleme yaklaşımı kullanmıştır. Belirlenen bu özellikler, BOTNET temel özellikleriyle yakından ilgili olması sebebiyle ANDROID cihazlardaki BOTNET saldırılarının tespit edilmesi mümkün olabileceğini değerlendirmiştir. Gorla ve ark. [14] çalışmasında ANDROID uygulama izin kullanımını analiz etmek için uygulama açıklamalarını ve kodlarını kullanmıştır. İlk olarak uygulamalar meta veri kullanımına göre sınıflandırmıştır. Aynı kümedeki uygulamalar API kullanımlarına göre analiz edilerek diğer uygulamalarla kıyaslamıştır. API yöntemlerini alışılmadık şekillerde kullanan uygulamalar şüpheli uygulama olarak işaretlemiştir. Bu çalışmada zararlı yazılım algılama oranları %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. Kılınç ve ark. [15] çalışmasında; kullanıcı bilgisayarlarının DDoS saldırısı amacıyla köle bilgisayar olarak kullanılıp kullanılmadığının belirlenmesi maksadıyla, makine öğrenimine dayalı sınıflandırma algoritmaları kullanmıştır. 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. Kılınç ve ark. mobil cihazlar hakkında pek fazla önerilerde bulunmamıştır. Özgür ve ark. [16] saldırı tespit sistemlerinde kullanılan kolay erişilen makine öğrenme algoritmalarının karşılaştırılması yapmış ancak yapılan çalışma veri setleri ve simülasyonlarda %90 üstünde sonuçlar vermiş olsa da gerçek bir ortamda aynı sonuçların verip veremeyeceği net değildir. Hoque ve ark. [17] çalışmasında, çeşitli BOTNET geliştirme araçları hakkında detaylı bir analize yer vermiş ve Mobil BOTNET saldırılarının karakteristikleri ayrıntısı ile analiz edilmiştir. Kandula ve ark. [18] Web sunucularını DDoS saldırılarına karşı korumak için istemcinin bir insan tarafından kontrol edilip edilmediğini belirlemek için grafiksel bir test olan Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA) kullanan bir sistem önermektedir. Kandula ve ark. tarafından önerilen grafiksel test yöntemi; WEB sitelerine karşı yapılan DDoS saldırılarının önlenmesinde güçlü bir bileşen olmuştur.

Ayrıca Yüksel ve ark. [19] sesin gerçek zamanlı olarak IP üzerinden iletilmesi Voice over IP (VoIP) için kullanılan Session Initiation Protocol (SIP) güvenlik açıklarını incelemiş ve çözüm yöntemleri önermiştir. Özellikle savunmasız sistemlerde uygulaması kolay olan DDoS hizmet kesintisi ve ortadaki adam saldırılarının gerçekleştirilmesi için gerekli olan yazılım ve araçlar incelenmiştir.

Gerçekleştirilen saldırıların sistemdeki olumsuz etkilerini en aza indirmek için ise, IDS/IPS olarak kullanılan yazılım ile çeşitli kurallar tanımlanmış ve saldırı anında alarm vermesi sağlanmıştır. Tek katmanlı bir güvenlik protokolünün kullanılması yerine tam koruma sağlanması için farklı katmanlarda farklı işlevleri olan güvenlik protokoller önerilmektedir. Çakır ve ark. [20] VoIP teknolojilerinde opnet tabanlı güvenlik uygulaması üzerine çalışmalar yapmış, bu sayede DDoS saldırılarında erişilebilirlik ilkesine bağlı kalarak hizmeti kısmi olarak devamlılığı sağlanmıştır. Ancak bilgisayar teknolojisinde olduğu gibi VoIP teknolojisi DDoS saldırılarına karşı yeterince güvenlik tedbirleri getirememiştir.

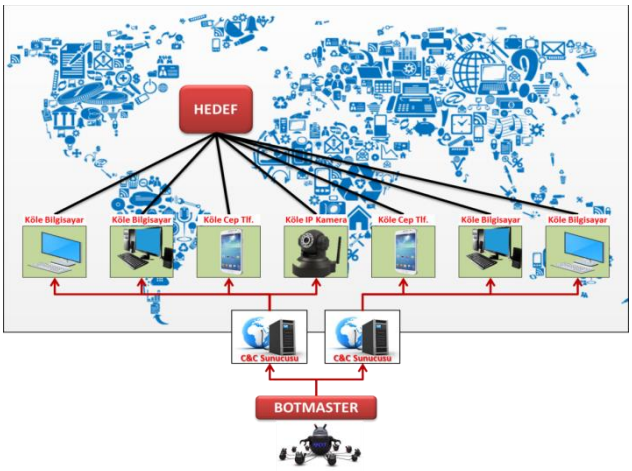
2012 yılından sonraki DDoS saldırılarında kullanılan cihazların sadece köle bilgisayarların olmadığı, zararlı yazılım bulaştırılmış akıllı telefon, IP kamera, IoT ve internete bağlı cihazlarında bu siber silahın bir parçası olduğu tespit edilmiştir. Bu çalışmada, Mobil BOTNET saldırılarının tanımı, hâlihazırda 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 arttırılması, cihazları üzerinde gerekli güvenlik güncellemeleri ve resmi olmayan uygulama mağazalarından elde edilmiş yazılımları daha dikkatli kullanılması sağlanacaktır.

3. DDoS SALDIRISI VE MOBİL BOTNET ÖZELLİKLERİ (DDoS ATTACKS AND FEATURES OF MOBİLE BOTNET)

Bu bölümde, DDoS saldırılarının genel tanımı ve hâlihazırda mevcut BOTNET ailelerinin DDoS maksadıyla kullanımı örnekler ile sunulmaktadır. Ayrıca BOTNET saldırılarının ortak özellikleri ve bu özelliklerle BOTNET modelleme adımları arasındaki ilişki anlatılmaktadır.

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

DDoS saldırılarına maruz kalan sistemin yanında ikincil kurbanlar; zararlı ya”zılım bulaştırılmış bilgisayar, akıllı telefon, IP kamera, IoT ve internete bağlı cihazlardır. Temel olarak tek bir IP adresinden yani sistemden gelen saldırılar donanımsal yâda 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 kullanılmaktadır. Köle bilgisayarlar zararlı yazılım geliştiricisi olan BOTMASTER tarafından yönetilmekte ve doğrudan BOTMASTER tarafından yönetilmez. Ara yönetim kademesi olarak Komuta ve Kontrol (C&C) Sunucuları” kullanılarak kendilerini çok rahatlıkla gizleyebilmektedir. Geliştirilen bu saldırı mimarisi ile hedef sunucu, web sayfası veya internet servis sağlayıcı dünyanın farklı yerlerindeki BOTNET’in bir parçası olmuş köle bilgisayar tarafından saldırıya maruz kalmaktadır. Şekil 1’de köle bilgisayar topluluğu ile yapılan bir DDoS saldırı senaryosu görülmektedir. Köle bilgisayar kullanıcıları bu yapının içinde olduğunun farkında değildir. Sadece bilgisayarının durduk yere yavaşlaması, internet bağlantısının sürekli paket göndermesi nedeniyle internet hızının düşmesi gibi durumlarda kullanıcılar tarafından fark edilebilmektedir. Kullanıcılar iyi bir anti-virüs ile kendi bilgisayarlarını incelediklerinde bu durumdan kurtulabilmektedirler.



Şekil 1. Köle bilgisayarlar ile yapılan DDoS atağı senaryosu [21]
(Scenario of DDoS attacks with BOTNET)

Geleneksel DDoS saldırısı; yüksek yoğunlukla, protokol tasarım hatalarını veya yazılım güvenlik açıklarını istismar için özel olarak tasarlanmıştır. Düşük yoğunluklu saldırılar (Low Rate Shrew DDoS), sistem kapasitesini veya hizmet kalitesini büyük ölçüde düşüren, ancak gizli bir davranış sergileyen ve algılama sistemlerinden kurtulabilen önemli bir değişken olarak ortaya çıkarmaktadır [22]. Şekil 2’deki saldırı istatistikleri incelendiğinde; 2012 yılından itibaren akıllı telefonlar, 2016 yılından itibaren nesnelerin interneti (IoT) BOTNET saldırıları amacıyla kullanılmasıyla, saldırı şiddetinin savunma sistemlerinin görevini yerine getiremeyecek boyutlara ulaştığı görülmektedir. Örneğin, 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 [23]. 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. Mevcut bilgi sistem altyapısı ile bir saniyede 1 Terabit boyutundaki DDoS saldırısına karşı bilgi sistem savunmasının yapılabilmesi neredeyse imkânsızdır. Bu durum; bir kişi veya grubun, dünya çapında bir siber silaha sahip olmasını sağlamaktadır. Tabi ki bu durumun oluşmasında en büyük etken, BOTNET teknolojisinin kendini geliştirmesi ve güvenlik boyutu göz arda edilerek üretilen IoT cihazlarıdır [24].

Şekil 2. DDoS Saldırı Boyutu [25]
(Size of DDoS attacks)

3.2. Mobil BOTNET Saldırılarının Özellikleri (Features of Mobile BOTNET Attacks)

Öncelikle BOTNET işlevselliğinin ortaya konulabilmesi için ortak özellikler belirlenmelidir. Diğer BOTNET saldırılarının tespitinde bu özellikler değerlendirilmelidir. Bu çalışmada BOTNET saldırılarına ait ortak özelliklerin belirlenemesi maksadıyla; son yıllarda yaygın ve 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 [26]. 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 3); zararlı yazılım paketlenmesi, uzaktan yönetim, e-posta veya SMS Okuma-Gönderme, veri hırsızlığı, ek içerik indirme/kurma, kök klasör (Root) saldırısı, üçüncü parti uygulama mağazaları ve uygulama izinleridir

Sıra Numarası		ZtorgB.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 3. Zararlı yazılım özelikleri
(Features of malware)

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

3.2.1. Zararlı Yazılımın Paketlenmesi (Packing of Malicious Software)

ANDROID ve iOS işletim sistemleri gibi diğer mobil işletim sistemleri kullanıcılarına resmi uygulama mağazalarından (Google Play Store, Samsung Apps ve Apple Store) uygulamaları indirme hizmeti sağlamaktadır. ANDROID işletim sistemi ayrıca resmi olmayan uygulama mağazaları ve sunuculardan uygulama kurulmasına izin vermektedir. BOTNET saldırı yönetimi zararlı yazılım kodları içeren uygulamalar sayesinde yapılabilmektedir. Orijinal uygulama kodu ters mühendislik işlemi yapıldıktan sonra zararlı yazılım kodu ilave edilerek yeniden paketlenir ve kullanıma sunulur. PjApps geleneksel BOTNET işlevselliğine sahip zararlı yazılım kod örneklerinden biridir. PjApps ilave edilmiş mobil uygulama yüklendiği cihaza bir arka kapı (Backdoor) açılmasına izin verir ve bu izinle uzaktaki sunucudan komut alınması sağlanır [27].

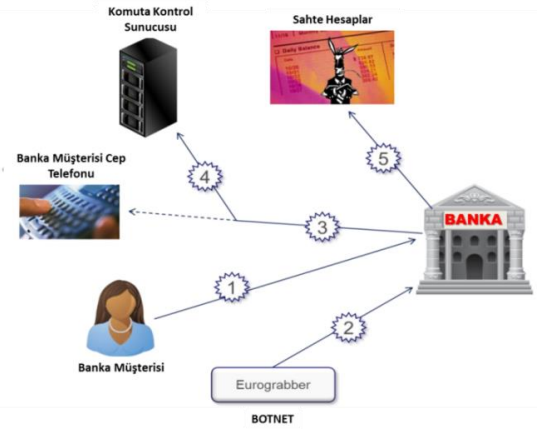
3.2.2. Uzaktan Yönetim (Remote Control)

BOTNET saldırılarının en önemli özelliklerinden birisi; uzaktaki bir sunucudan komutlar alabilmesidir. BOTMASTER komutlarını hedef cihazlara göndermek ve yanıt almak için C&C ara yüzünü kullanır [28]. Mobil BOTNET saldırılarında kullanılan güncel teknikler ile geleneksel teknikler birbirine çok benzemektedir. Bazı durumlarda komutlar doğrudan C&C sunucusundan BOT'a gönderilir bazen ise BOT'un düzenli aralıklarla C&C sunucusuyla iletişime geçmesine izin verilir ve yeni komutların mevcut olup olmadığı sorgulanır. Örnek olarak AnserverBot BOTNET'i incelendiğinde; virüs bulaşmış cihazdaki güvenlik çözümünü tespit etme ve devre dışı bırakmanın yanı sıra, kendini her türlü değişiklikten korumak için bütünlük doğrulama imzasını kontrol eder. TigerBot ise web teknolojisi yerine SMS ile kontrol edilen bir BOTNET'dir. C&C mesajlarını algılar ve onları mobil cihaz sahiplerinden gizler. SMS

mesajlarını kendi sunucusunda toplamak yerine, telefon görüşmelerini veya telefon görüşmesi olmadığı zamanlarda ortamdaki sesleri kaydeder.

3.2.3. E-posta ve SMS Okuma-Gönderme (Messaging)

Geleneksel BOTNET saldırısının temel amacı maddi kazanç sağlamaktır. Bu BOTNET'ler; normal telefon hatlarına göre daha yüksek ücret tarifesine sahip ücretli hatlara düzenli aralıklarla gizlice SMS göndererek ciddi maddi kayıplara neden olmaktadırlar. RootSmart/Bmaster ücretli hatlara SMS göndererek milyonlarca dolar haksız kazanç sağlamıştır. 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 amacıyla geliştirdikleri tek kullanımlık SMS şifresini çalmak suretiyle müşterilere ait bankacılık işlemlerine ulaşmaktadır. Bu yöntemle Avrupa'daki bankalardan 2012 yılında 36 Milyon Euro çalınmıştır [29]. Zitmo zararlı yazılımı çalışma yöntemi Şekil 4'de gösterilmiştir.



Şekil 4. Zitmo zararlı yazılımı çalışma yöntemi [29]
(Zitmo malware work method)

ESET güvenlik firması tarafından Şubat 2017'de Spy.Banker.HU adıyla etiketlenen zararlı yazılım, yaygın olarak kullanılan hava durumu uygulaması Good Weather içersinde kendisini gizleyerek 22 Türk Banka müşterisini hedef almıştır. ANDROID işletim sistemi uygulama mağazasıdan (Google Play Store) indirilebilen bu uygulamanın iki farklı sürümü vardır. ESET firmasının uyarısı üzerine zararlı yazılım içeren Good Weather Google Play Store'dan kaldırılmıştır. Uygulama mağazasında çok kısa bir süre yer almasına rağmen kullanıcılar tarafından binlerce kez indirilmiştir. İlk tespitlere göre 48 farklı ülkede 5 bin kullanıcıya etkilenmiştir (Şekil 5). Söz konusu uygulama yüklendikten sonra hava durumu görünümlü ikon önce kaybolmakta, sonrasında kullanıcıdan yönetici haklarını talep eden bir mesaj görünmektedir. Eğer kullanıcı tarafından bu mesaj onaylanırsa, zararlı yazılıma kilit ekranı parolasını değiştirme ve ekranı kilitleme yetkisi verilmektedir. Bu yetkilerle birlikte SMS mesajlarına da ulaşabilme imkânı alan zararlı uygulamanın önünde hiçbir engel kalmamaktadır. Kullanıcılar tarafından güzel bir hava durumu uygulaması yüklenildiği düşünülürken, arka planda çalışan zararlı uygulama, elde ettiği SMS ve bankacılık bilgilerini C&C sunucularına dolayısıyla siber hırsızlara iletmektedir [30].

Şekil 5. Virüs içeren hava durumu uygulaması kullanıcı durumu [30]
(Status of infected weather application users)

3.2.4. Veri Hırsızlığı (Data Theft)

Siber saldırganlar elde ettikleri kişisel verileri uzaktaki bir sunucuya gönderirler. Bu husus zararlı uygulamanın cihaza kurulumundan sonra gerçekleşir. Genel olarak 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 fotoğraflar saldırganlar tarafından ele geçirilmesi arzulanmaktadır. Geinimi geleneksel BOTNET işlevlerini sergileyen zararlı bir yazılımdır [31]. Bu zararlı yazılım, cihazdaki kişisel verileri toplar ve bu bilgiyi uzaktaki bir sunucuya iletir. TigerBot.A ve PjApps.A zararlı yazılımları mobil cihazlara ait IMEI, telefon numarası ve SMS bilgilerini toplar ve uzaktaki bir sunucuya gönderir. 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 [32]'de sunulmuştur.

3.2.5. Ek İçerik İndirme/Kurma (Additional Content Downloading/Installing)

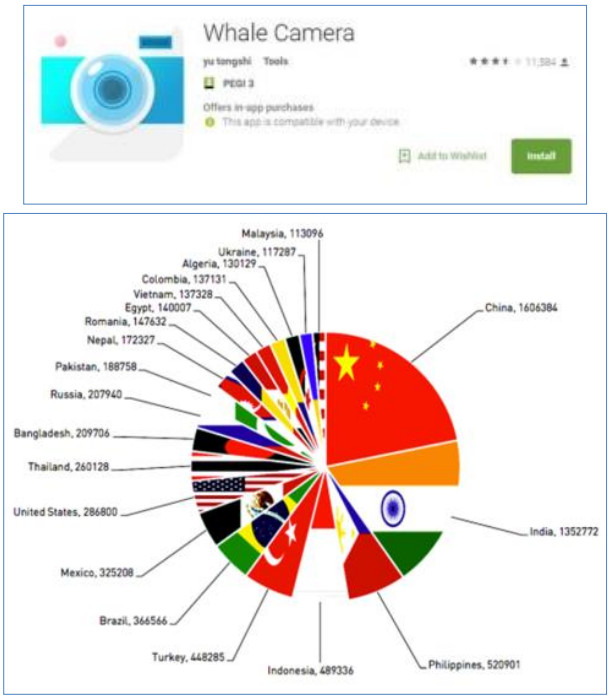
Mobil BOTNET saldırılarının en yeni özelliklerinden birisi zararlı yazılım bulaşmış akıllı telefonlarda,

kullanıcının bilgisi dışında cihazlara ek içerik indirilebilmesidir. Bu içerik, özellikle zararlı yazılım kodları ile ilgili olup, BOTNET saldırısının cihaz içindeki hareket kabiliyetini artırır. Bu içerikler kullanıcının yanlış yönlendirilmesi ile gerekli indirme işlemini yapması veya bilgisi dışında indirilmesi gerçekleşir. 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.

3.2.6. Kök Klasör Saldırısı (Root Exploit)

Bazı Mobil telefon kullanıcıları mevcut mobil işletim sistemi daha fazla hareket kabiliyeti ve yazılım yetkisi elde edebilmek için ROOT yetkisi üzerinde değişiklikler yapmaktadır. RootSmart/Bmaster zararlı yazılımı, bazı ANDROID işletim sistemi sürümlerinde 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 oluşturmuştur [33].

Google Play Store'da bulunan 20'den fazla uygulamada HummingBad zararlı yazılımının yeni bir çeşidi Check Point firması tarafından Kasım 2016 tarihinde tespit edilmiştir. Virüsten etkilenen bu uygulamalar hiçbir şeyden haberi olamayan kullanıcılar tarafından milyonlarca kez indirilerek cihazlarına yüklenmiştir [34]. Söz konusu zararlı yazılımı Google Play Store'dan kaldırılmasına rağmen 10 milyondan fazla cihazın bu virüsten etkilendiği değerlendirilmektedir (Şekil 6) [35].



Şekil 6. Virüs içeren uygulamaların kullanıcı durumu [35]
(Status of infected application)

3.2.7. Üçüncü Parti Uygulama Mağazaları (Third Party Application Stores)

Google Play Store, Galaxy App, ANDROID Market, Apple Store ve BlackBerry App World gibi resmi uygulama mağazaları mobil işletim sistemleri için en temel uygulama yükleme noktalarıdır. ANDROID işletim sistemi bunun dışında üçüncü parti uygulama mağazaları veya forum sitelerinden ücretli veya ücretsiz uygulamaların yüklenmesine müsaade etmektedir. Üçüncü parti uygulama mağazaları resmi uygulama mağazalarında bulunmayan birçok özellik sunmaktadır. Örneğin ücretli veya reklam içerikli uygulamalar ücretsiz olarak tam sürümleri ile birlikte sunulmaktadır. Ancak bu uygulamaların birçoğu zararlı yazılım içermektedir.

3.2.8. Uygulama İzinleri (Permissions)

ANDROID işletim sistemi hassas kaynak ve işlemlere erişimi uygulama izinleri ile tanımlar. Hali hazırda ANDROID işletim sisteminde tanımlı 137 uygulama izninin [36] 122 tanesi üçüncü parti uygulamalar için kullanılabilmektedir [37]. İzinler ANDROID işletim sisteminde AndroidManifest.xml dosyasında tanımlanmaktadır. Yüklenen uygulamaların güvenlik riskleri hakkında kullanıcıları bilgilendirme bu izinler sayesinde yapılmaktadır [38]. Ancak ANDROID izin bildirimlerinin çoğunlukla kullanıcılar tarafından göz ardı edildiği veya hiç dikkate alınmadan uygulamanın yüklendiği tespit edilmiştir [39, 40]. Örneğin, hava durumu bilgisi almak için yüklenen basit bir uygulama, telefonumuzdaki birçok yetkiye (Kamera, GPS, mikrofon, rehber, hafıza erişimi vb.) sahip olabilmektedir. Söz konusu uygulama izinlerinin kullanıcılar tarafından düzenlenmesi ANDROID 6.0 Marshmallow sürümü ve sonrasında geliştirilmiştir. Daha önceki sürümlerde bu yetki kullanıcılara verilmemiştir. Şekil 7'da sunulan tabloda görüldüğü gibi kullanıcıların %42.3'ü kullandığı uygulama izinlerini düzenleyemeye yetkisi bulunmamaktadır. Bu durum ise zararlı yazılım içiren uygulama geliştiricileri tarafından istismar edilmektedir.

Sürüm Numarası	Android Sürümü	Kullanım Oranı	Uygulama Yetki Kısıtlama
2.3.3	Gingerbread	0.3%	Yok
4.0.3	Ice Cream Sandwich	0.4%	
4.0.4			
4.1.x	Jelly Bean	1.7%	
4.2.x		2.6%	
4.3		0.7%	
4.4	KitKat	12.0%	
5.0	Lollipop	5.4%	
5.1		19.2%	
6.0	**Marshmallow**	**28.1%**	Var
7.0	**Nougat**	**22.3%**	
7.1		**6.2%**	
8.0	**Oreo**	**0.8%**	
8.1		**0.3%**	

Şekil 7. ANDROID sürümleri kullanım oranları [36]
(Usage rates of ANDROID OS versions)

Bu bölümde anlatılan BOTNET ortak özellikleri sayesinde yapılabilecek saldırılar hakkında fikir sahibi olunmaktadır. Zararlı yazılımın neden bir bilgisayara veya akıllı cihaza erişme-yayılma politikasının devam ettirdiği bu özellikler sayesinde ortaya çıkmaktadır. Tek bir IP'den yapılan saldırı IP adresi yasaklanarak engellenebilir. Ama bu durumun yüz binlerce ve dünyanın farklı noktalarından aynı anda yapılan bir saldırı olarak ortaya çıkmasında, alınan emniyet tedbirlerinin çok güçlü olmadığı durumlarda saldırı amacına ulaşmaktadır. Amaçlanan servis dışı bırakma işlemi gerçekleşmiş olur. Siber silahın bir parçası olan DDoS saldırısı ancak BOTNET ordusundaki BOT'ların sayısı ve çeşitliliği (PC, Akıllı Cihaz, IP Kamera, lOT vb.) ile güçlenmektedir. BOTNET temel özelliklerinden; uzaktan yönetim, zararlı yazılım paketlenmesi, uygulama izinler ve üçüncü parti uygulama mağazalarından yayılma en temel özelliklerdir. 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.

4. ANALİZ (ANALYSIS)

Bu bölümde, DDoS bir unsuru olarak kullanılan Mobil BOTNET Geliştirme Modeli, BOTNET tespit yönteminin analizi, tersine mühendislik yönteminin kullanımı ve ANDROID izinlerini inceleme yöntemi hakkında bilgi verilmektedir. Bu doğrultuda mobil cihaz kullanıcıları tarafından yapılması gereken hususlar önerilmiştir.

4.1. Mobil BOTNET Geliştirme Modeli (Mobile BOTNET Development Model)

Varlığı ilk olarak 2010 yılında keşfedilen mobil BOTNET saldırılarının siber dünyadan kaldırılması neredeyse imkânsız hale gelmiştir. Bu zararlı yazılımların yeni sürümleri hedef cihazdaki komutları çalıştırmak için birden fazla C&C sunucusu kullanmaktadır. BOTNET saldırısında bilgisayar korsanları tarafından ele geçirilen kişisel verilerin şantaj, casusluk veya maddi kazanç sağlamak maksadıyla kullanılabilmesi, bu saldırıların neden siber uzayın vazgeçilmez bir silahı olduğunu açıklamaktadır. Mobil cihazların DDoS saldırılarında kullanıldığı gerçeği dikkate alındığında bu cihazlara yönelik geliştirilen farklı uygulamalar bulunmaktadır. Bu güvenlik uygulamalarının ücretli olması veya mobil cihaz kullanıcıları tarafından tehlikenin tam olarak anlaşılamaması nedeniyle yaygın olarak kullanılmamaktadır. Uygulama geliştiricilerinin arz-talep dengesini dikkate alması ve bu alandaki pazar payının istenen seviyeye gelmemesi nedeniyle, mobil cihaz güvenliği masaüstü bilgisayarlar güvenliğine nazaran ilk evrelerini yaşamaktadır.

Bir mobil uygulamanın zararlı yazılım içerip içermediğini veya BOTNET işlevlerine sahip olup olmadığını öğrenmek için, bir önceki bölümde açıklanan özellikleri algılama yöntemleri kullanılabilir. Şekil 8'de gösterilen Mobil BOTNET Geliştirme Modeli (BOTMASTER'ın bir BOTNET saldırısını geliştirme aşamaları) ve BOTNET saldırısının özelliklerinin hangi aşamalarda ortaya çıktığı anlatılmaktadır.

Şekil 8. Mobil BOTNET geliştirme modeli
(Mobile BOTNET development model)

BOTNET saldırısını oluşturulma süreci, BOTMASTER tarafından BOT koduna yer açmak için meşru bir uygulamayı değiştirmesi ile başlar [41]. Bulaşma evresinde; bir uygulamanın işlemini, yapısını ve işlevlerini öğrenmek amacıyla uygulamanın tekrardan kaynak kodlarına ulaşılması olarak tanımlanan tersine mühendislik yöntemi kullanılır. İlk olarak orijinal uygulamanın kaynak kodu ApkTool, Dex2Jar, Notepad++, AndroGuard vb. araçlar ile elde etmektedir [42]. Orijinal uygulama kodlarına zararlı uygulama içerikleri ilave edilmesi ile BOTNET ortak özelliği olan Zararlı Yazılım Paketlenmesi bu evrede gerçekleşmiş olur.

Mobil BOTNET Geliştirme modelinin ikinci aşamasında; zararlı kod ile yeniden paketlenmiş uygulamaya mobil cihazlara dağıtılması hedeflenmektedir. Bu uygulamaların yeterli sayıda mobil cihaza bulaşmaması, büyüme yeteneğini kaybetmesi anlamına gelir ve DDoS maksadıyla kullanımını engeller. Zararlı kod ihtiva eden uygulama e-posta, dosya paylaşımı, üçüncü parti uygulama internet siteleri, ücretsiz veya zararlı URL'ler vasıtasıyla yayılmaktadır [43]. En yaygın ve etkili yayma yöntemi olan üçüncü parti uygulama internet sitelerine BOTMASTER tarafından zararlı yazılım içeren yeniden paketlenmiş uygulama yüklenerek ikinci aşama gerçekleştirilmiş olur. Bu aşama, yedinci BOTNET ortak özelliğini (Üçüncü Parti Uygulama Mağazası) ortaya çıkarır.

Mobil BOTNET Geliştirme Modeli'nin son aşaması BOTNET saldırısının amacına ulaşacağı Uygulama safhasıdır. Uzaktan Yönetim, Eposta veya SMS Okuma-Gönderme, Veri Hırsızlığı, Ek İçerik İndirme/Kurma ve Kök Klasör Saldırısı gibi BOTNET'in diğer temel özellikleri bu safhada ortaya çıkmaktadır.

4.2. BOT Tespit Yöntemleri (BOT Discovery Methods)

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.

4.2.1. Tersine Mühendislik Yöntemi (Reverse Engineering Method)

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 uygulama dosyaları orijinal kaynak kodlarına ApkTool, Dex2Jar, Notepad++, AndroGuard vb. araçlar kullanılarak ulaşılmaktadır. BOTNET Keşif Süreci bir güvenlik analistinin belirli bir uygulamanın BOTNET saldırıları ile ilgili olarak zararlı olup olmadığını belirlemek için izleyebileceği adımları açıklar [44]. Tersine mühendislik sayesinde kaynak kodlarının her satırı incelenir ve zararlı yazılım içerip içermediği tespiti edilir. Ancak güvenlik uygulamasının binlerce kod satırını değerlendirmesi çok zaman alıcı bir uygulamadır. Ancak BOTNET ortak özelliklerinin, mobil BOTNET'in tespitinde kullanılması zararlı yazılım koduna kısa sürede tespit edilmesine yardımcı olabilir.

4.2.2. ANDROID İzinlerini İnceleme Yöntemi (Analysis of ANDROID OS Permissions Method)

Zararlı kod içeren uygulamanın tespiti için ilk önce güvenlik uzmanı tarafından uygulamanın yeniden paketlenmiş bir uygulama olup olmadığı belirlenmelidir [45]. Yeniden paketlenmiş uygulamalar uygulama izinlerinin kayıt altına aldığı AndroidManifest.xml dosyası incelenerek belirlenebileceği gibi 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.

Söz konusu uygulama izinlerinin orijinal uygulamanın bir parçası olarak tanımlanabileceği gerçeği göz önüne alındığında, bu alt küme ANDROID izinlerinin tanımlanmış olması bir tehdide atıfta bulunmaz. Ancak güvenlik uzmanları uygulamaya ait tüm kod yapılarını değerlendirmek yerine yalnızca yukarıda belirtilen özelliklerle ilgili anahtar kod taraması yapması süreci kısaltmaktadır. Ayrıca BOTNET temel özellikleri ve algılama mekanizmalarının incelenmesi ne kadar değerli olsa da, en güvenilir yöntem orijinal uygulama mağazaların kullanılmasıdır.

4.2.3. Kullanıcı Tarafından Alınması Gereken Önlemler (Precautions to be Taken by the User)

Bir DDoS saldırısının hedefi kullanıcılar değildir. Kullanıcı cihazları sadece hedefe ulaşmak için kullanılan birer araçtır. Farkında olmadan bir BOTNET'in parçası olarak bir DDoS saldırısına katılıyor olabilir miyiz? Bunun farkına nasıl varabiliriz? gibi soruların cevaplarını kullanıcılar kendi cihazlarında yapması gereken birkaç işlem sayesinde bulabilir.

a) En önemli husus uygulamaların resmi uygulama mağazalarından yüklenmesi ve BOTNET'in yedinci temel özelliği olan üçüncü parti uygulama mağazalarına ait uygulamalardan uzak durulmasıdır. Üçüncü parti uygulama mağazalarına ait uygulamalar temel olarak BOTNET özelliklerini taşıması ve zararlı kod ile yeniden paketlenme olasılığı nedeni ile çok tehlikelidir.

b) Mobil cihazlardaki güvenlik açıkları üretici firmalar tarafından yayınlana güncellemeler ile kapatmaktadır. Kullanıcılar tarafından gereksiz veri kaybı veya güncelleme sonrasında mobil cihazın yavaşlayabileceği kanısı bu güncellemeleri ertelemesine neden olmaktadır. Buna kanıya rağmen kullanıcılar mobil cihaz güvenlik güncellemelerini mutlaka takip edilmeli ve cihazlarını güncel tutmalıdır.

c) Uygulamaların zararlı yazılım içerip içermediği anti-virüs programı ile denetlenmeli ve anti-virüs uygulamasına ait veri tabanını sürekli güncel tutulmalıdır.

d) Mobil cihazlardaki internet paketi işlem yapılmadığı halde çok çabuk sürede bitiyorsa, cihazda zararlı yazılım olabileceği ve arka planda bir saldırının parça olabileceği değerlendirilmelidir. Telefon ayarlarından uygulamalara ait internet kullanımı bilgisi incelenmeli ve arka planda aşırı internet kullanımı yapan uygulamalardan mutlaka şüphe duyulmalıdır.

e) DDoS saldırısının bir parçası olmamak için; uygulamalara ait arka plan veri kullanımı ihtiyaç duyulmadığı zamanlarda kapatılmalıdır.

f) Bütün bu işlemler yapıldıktan sonra dahi cihazın BOT olarak kullanıldığından şüpheleniliyorsa, mutlaka iyi bir yedek aldıktan sonra fabrika ayarlarına geri dönülerek içindeki bütün bilgiler silinmelidir.

g) ANDROID 6.0 ve sonrası sürümleri kullanan sahip cihazlardaki uygulamalara ait standart izinler kontrol edilerek gereksiz izinler kapatılmalıdır. Yeni tehditleri tanımlamak ve güvende kalmak için anti-virüs ve mobil güvenlik uygulamaları düzenli olarak mutlaka güncellenmelidir.

5. SONUÇ (CONCLUSION)

Akıllı mobil cihazlar dünyadaki milyarlarca insanın kullandığı bir teknolojidir. Mobil cihazların internet, konum belirleme sistemleri (GPS), kablosuz iletişim ve sağlık uygulamaları gibi ileri düzey yetenek ve teknolojilerinin gelişimiyle kullanım oranları artmıştır. Büyük bir kullanım yelpazesine sahip olması, kullanım oranın artması ve güvenlik açısından henüz gelişme döneminde olması sebebiyle mobil işletim sistemlerine sahip cihazlar zararlı yazılım geliştiricilerin hedefi haline gelmiştir. Aslında bir çok hassas veri, iletişim bilgisi, şifre hatta kredi kartı numaraları bu küçük cihazlarda tutulmaktadır.

Bu çalışmada, Mobil BOTNET'in DDoS saldırısında nasıl kullanılabileceği araştırılmış, BOTNET saldırılarının ortak özellikleri ve BOTNET modelleme adımları arasındaki ilişki saptanmış, uygulamalarda söz konusu özelliklerin tespit yöntemleri ile BOTNET saldırılarınan korunmak için önerilerde bulunulmuştur.

Elde edilen bulgular;

• 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 2012 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,

• BOTNET ve DDoS saldırıları hakkında mobil cihaz kullanıcılarının bilgi sahibi olmadığı ve yapılan bu çalışmanın bu farkındalığı artıracağı tespit edilmiştir.

Sonuç olarak; ANDROID işletim sistemlerinde resmi olmayan çok sayıda uygulama mağazasının bulunması, kullanıcıların uygulamaları bu mağazalardan indirip yükleyebilmesi ve iki yılını dolduran cihazlara firmalar tarafından güncelleme desteğinin kesilmesi güvenlik riskini artmıştır. Bu durum, BOTNET'lerin ANDROID işletim sistemi için büyük bir soruna dönüşmesine ve DDoS maksadıyla rahatlıkla kullanılmasında sebebiyet vermektedir.

Hedefli ve koordine bir şekilde gerçekleştirilen ve mobil cihazlarla desteklenen DDoS atakları geleneksel savunma metotlarının gücünü zayıflatmaktadır. Mevcut internet ve DNS altyapısı bu atakların engellemesinde yetersiz kalmaktadır. Mobil BOTNET ve DDoS saldırılarına istemsiz isteklerin engellenmesi ve tespiti maksadıyla mutlaka CAPTCHA yönteminin kullanımı yaygınlaştırılmalıdır. Özellikle finans, sağlık ve şehir altyapı sistemlerine hizmet veren birimler için benzer sunucu yapısı kapsamında yeni yaklaşım ve metotların geliştirilmesine ihtiyaç vardır.

KAYNAKLAR (REFERENCES)

[1] P.W. Singer, A. Friedman, **Cybersecurity And Cyberwar**, 14-15, 2014.

[2] M. Gürkaynak, "Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler", Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 16(2), 264, 2011.

[3] United States of America Department of Defense, **Department of Defense Dictionary of Associated Terms**, Joint Chiefs of Staff, 93, 2010.

[4] M.G. Todd, **Armed Attack In Cyberspace: Deterring Asymmetric Warfare With Asymmetric Definition**, Air Force Law Review (65), 64-69, 2009.

[5] Internet: Elektrik neden kesildi? Türkiye genelinde elektrik kesintisi, http://www.ntv.com.tr/turkiye/elektrik-neden-kesildi-turkiye-genelindeelektrik-kesintisi,RhfwqMiN NkOUj5_sO12qJg, 28.02.2018.

[6] S.W. Brenner, M.D. Goodman, "In Defense of Cyberterrorism: An Argument for Anticipating Cyber-Attacks", University of Illinois, Journal of Law, Technology& Policy, 1-57, 2002.

[7] Y. Xiang, W. Zhou, M. Chowdhury, "A Survey of Active and Passive Defence Mechanisms against DDoS Attacks", Deakin University, School of Information Technology, 51 (2), 2004.

[8] C. Douligeris, A. Mitrokotsa, "DDoS Attacks and Defense Mechanisms: Classification and State-of-the-Art", Computer Networks, 44(5), 643-666, 2003.

[9] BİLGEM, DDoS ile Mücadele Kılavuzu, 2015.

[10] A.R. Flo, A. Josang, "Consequences of BOTNETs Spreading to Mobile Devices", **14th Nordic Conference on Secure IT Systems**, Oslo, 2009.

[11] İnternet: Worldwide Smartphone Growth Goes Flat in Q1 2016, Apple Market Share Drops to 15.3%, http://www.iclarified.com/54990/worldwide-smartphone-growth-goes-flat-in-q1-2016-apple-market-share-drops-to-153-chart, 17.02.2017.

[12] J.S.Lee, H. Jeong, J. H. Park, M. Kim, B.N. Noh, "The Activity Analysis of Malicious HTTP-Based BOTNETs Using Degree of Periodic Repeatability", **International Conference on Security Technology**, 83-86, 2008.

[13] S. Joshi, R. Khanna, L.K. Joshi, "ANDROID BOTNET: An Upcoming Challenge", **National Conference on Advances in Engineering (Technology & Management)**, 5-10, 2015.

[14] A. Gorla, I. Tavecchia, F. Gross, A. Zeller. "Checking App Behavior against App Descriptions.", **36th International Conference on Software Engineering**, 1025-1035, 2014.

[15] D. Kılınç, F. Bozyiğit, E. Borandağ, F. Yücalar, H. Akyol, E. B. Akırmak, Z. Uzun, "Sınıflandırma Tabanlı Zombi Bilgisayar Tespit Sistemi", **Akademik Bilişim 2016**, Adnan Menderes Üniversitesi, Aydın, Şubat, 2016.

[16] A.Özgür, H. Erdem, "Saldırı Tespit Sistemlerinde Kullanılan Kolay Erişilen Makine Öğrenme Algoritmalarının Karşılaştırılması", Bilişim Teknolojiler Dergisi, 5(2), 41-48, 2012.

[17] N. Hoque, D. K. Bhattacharyya, J. K. Kalita, "BOTNET in DDoS Attacks: Trends and Challenges", IEEE Communication Surveys & Tutorials, 17(4), 2243-2269, 2015.

[18] S. Kandula, D. Katabi, M. Jacob, A. Berger, "Botz-4-sale: Surviving Organized DDoS Attacks That Mimic Flash Crowds", **2nd Symposium on Networked Systems Design & Implementation**, 287-300, 2005.

[19] M. Yüksel, N. Öztürk, "SIP Saldırıları ve Güvenlik Yöntemleri", Bilişim Teknolojiler Dergisi , 10(3), 301-310, 2017.

[20] C. Çakır, H. Kaptan, "VoIP Teknolojilerinde Opnet Tabanlı Güvenlik Uygulaması", Bilişim Teknolojiler Dergisi, 2(3), 1-7, 2009.

[21] R.K.C. Chang, Defending Against Flooding-Based, Distributed Denial of Service Attacks: a Tutorial, IEEE Communications Magazine 40, 42-51, 2002.

[22] Y. Chen, YK. Kwok, K. Hwang, "Filtering Shrew DDoS Attacks Using A New Frequency-Domain Approach", **1st IEEE LCN Workshop on Network Security**, Sydney, 2005.

[23] STM, **Ekim-Aralık 2016 Siber Tehdit Durum Raporu**, STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş, Türkiye, 2017.

[24] İnternet: IoT-Powered DDoS Attacks and SCADA Incidents Will Make Top Security Headlines in 2017 Bitdefender predicts https://businessinsights.bitdefender.com/iot-DDoS-attacks-scada-incidents, 01.03.2018.

[25] ARBOR, **Arbor Networks Special Report**, 12, 34, 2017.

[26] İnternet: Current ANDROID malware, http://forensics. spreitzenbarth.de/ ANDROID-malware, 19.02.2018.

[27] İnternet: C. A. Castillo, ANDROID malware past, present, and future, https://pdfs.semanticscholar.org/5735/6502310474b a9564ec8f581494b8de50b3e5.pdf, 22.02.2018.

[28] M. Eslahi, R.Salleh, N.B Anuar, "MoBots: A New Generation of BOTNETs on Mobile Devices and Networks", **International Symposium on Computer Applications and Industrial Electronics (ISCAIE)**, 262-266, 2012.

[29] İnternet: Eurograbber SMS Trojan steals €36 million from online banks,http://www.techworld.com/news/security/eurograbber-sms-trojan-steals-36-million-from-online-banks-3415014, 19.02.2018.

[30] İnternet: Released ANDROID Malware Source Code Used to Run a Banking Botnet, http://www.welivesecurity.com/2017/02/23/ released-ANDROID-malware-source-code-used-run-banking-botnet/, 25.02.2018.

[31] N.B. Thakkar, "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, 2015.

[32] R.P. Minch, "Privacy Issues in Location-Aware Mobile Devices", **37th Annual Hawaii International Conference on System Sciences**, USA, 2004.

[33] Y. Zeng, **On detection of current and next-generation BOTNETs**, Doktora Tezi, University of Michigan, Computer Science and Engineering, 2012.

[34] İnternet: A Whale of a Tale: HummingBad Returns, http://blog.checkpoint.com/2017/01/23/hummingbad-returns, 17.02.2018.

[35] İnternet: 10 Million ANDROID Phones Infected by All-Powerful Auto-Rooting Apps, https://arstechnica.com/security/ 2016/07/virulent-auto-rooting-malware-takes-control-of-10-million-ANDROID-devices/, 27.02.2018.

[36] İnternet: Manifest Permission List, https://developer. ANDROID.com/reference/ANDROID/Manifest.permission.html, 25.02.2018.

[37] K. W. Y. Au, Y. F. Zhou, Z. Huang, P. Gill, and D. Lie, "A Look At Smartphone Permission Models", **CCS'11 the ACM Conference on Computer and Communications Security**, 63–68, 2011.

[38] İnternet: A Guide to Understanding ANDROID App Permissions (& How to Manage Them), http://www.hongkiat.com /blog/ANDROID-app-permissions/, 28.02.2018.

[39] A. P. Felt, K. Greenwood, D. Wagner, "The Effectiveness of Application Permissions", **2nd USENIX Conference on Web Application Development**, 75-86, 2011.

[40] W. Enck, M. Ongtang, and P. McDaniel, "On lightweight Mobile Phone Application Certification", **16th ACM Conference on Computer and Communication Security**, New York, 235-245, 2009.

[41] M. Bailey, E. Cooke, F. Jahanian, X. Yunjing, and M. Karir, "A Survey of BOTNET Technology and Defenses", **Cybersecurity Applications & Technology Conference for Homeland Security**, 299-304, 2009.

[42] Vibha Manjunath, **Reverse Engineering of Malware on ANDROID**, Yüksek Lisans Tezi, University of ESSEX, 2011.

[43] N. Hachem, Y.B. Mustapha, G.G. Granadillo, H. Debar, "BOTNETs: Lifecycle and Taxonomy", **Conference on Network and Information Systems Security**, France, 1-8, 2011.

[44] H. Pieterse, M. S. Olivier, "ANDROID BOTNETs on the rise: Trends and characteristics", **Conference on Information Security for South Africa**, South Africa, 1-5, 2012.

[45] W. Zhou, Y. Zhou, X. Jiang, P. Ning, "Detecting Repackaged Smartphone Applications in Third-Party ANDROID Marketplaces", **2nd ACM Conference on Data Application Security and Privacy**, San Antonio, USA, 317-326, 2012.