TOBB EKONOMİ VE TEKNOLOJİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

TÜRKİYE'DE VE AVRUPA'DA DRDOS YÜKSELTİCİLERİNİN ANALİZİ

YÜKSEK LİSANS TEZİ

Emre Murat ERCAN

Bilgisayar Mühendisliği Anabilim Dalı

Tez Danışmanı: Prof. Dr. Ali Aydın SELÇUK

AĞUSTOS 2019

Fen Bilimleri Enstitüsü Onayı

Prof. Dr. Osman EROĞUL
Müdür

Bu tezin Yüksek Lisans derecesinin tüm gereksinimlerini sağladığını onaylarım.

Prof. Dr. Oğuz ERGİN
Anabilimdalı Başkanı

TOBB ETÜ, Fen Bilimleri Enstitüsü'nün 141111058 numaralı Yüksek Lisans Öğrencisi **Emre Murat ERCAN** 'ın ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı **"Türkiye'de ve Avrupa'da DRDoS Yükselticilerinin Analizi"** başlıklı tezi **08, Ağustos, 2019** tarihinde aşağıda imzaları olan jüri tarafından kabul edilmiştir.

Tez Danışmanı : **Prof. Dr. Ali Aydın SELÇUK**
TOBB Ekonomi ve Teknoloji Üniversitesi

Jüri Üyeleri : **Doç. Dr. Ahmet Burak CAN (Başkan)**
Hacettepe Üniversitesi

Dr. Mücahid KUTLU
TOBB Ekonomi ve Teknoloji Üniversitesi

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, alıntı yapılan kaynaklara eksiksiz atıf yapıldığını, referansların tam olarak belirtildiğini ve ayrıca bu tezin TOBB ETÜ Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırlandığını bildiririm.

ÖZET

Yüksek Lisans

Türkiye'de ve Avrupa'da DRDoS Yükselticilerinin Analizi

Emre Murat ERCAN

TOBB Ekonomi ve Teknoloji Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Prof. Dr. Ali Aydın SELÇUK

Tarih: Ağustos 2019

Hizmet engelleme saldırıları geçmişten günümüze değişik stratejiler ile etkinliğini artırarak devam etmektedir. Dağıtık Yansıtılmış Hizmet Engelleme Saldırısı (DRDoS) diğer adı ile Yükseltme Saldırısı, hizmet engellemeye yönelik saldırı türlerindeki yeni eğilimdir. Saldırganlar, Dağıtık Yansıtılmış Hizmet Engelleme saldırılarında genellikle UDP protokolü kullanan servisleri yansıtıcı olarak kullanırlar. Saldırganın sahip olduğu BotNetler kurbanın IP adresini taklit eder ve UDP tabanlı servislere sorgu gönderir. Sunucular tarafından oluşturulan yanıtlar kurbana gider ve bu şekilde kurbanın verdiği hizmetin geçici olarak devre dışı bırakılmasına ya da çok büyük gecikmeler ile verilmesini sağlar. Saldırganlar tarafından yapılan bu sorgularda saldırı verimini artırabilmek amacıyla genel olarak büyük miktarda cevap verisi üretecek sorgular tercih edilir. NTP, DNS ve memcached hizmetleri yüksek oranlı cevap verisi oluşturan protokollerden bazılarıdır.

Saldırıların gücü internet üzerinde bulunan yansıtıcı sayısı ile de doğru orantılıdır. Saldırıların etkinliğinin azaltılabilmesi dolaylı olarak tüm UDP tabanlı çalışan sunucu yöneticilerinin de elindedir.

Sunucuların bilinen zafiyetlerini kapatmak, saldırılarda yükseltici ya da diğer bir tabir ile yansıtıcı olarak kullanılmalarının önüne geçecektir. Hali hazırda DRDoS saldırıları sırasında kullanılan birçok servis için sıkılaştırma yöntemlerinin belirlenmiş olmasına karşın, internet üzerinde çok sayıda yansıtıcı bulabilmek mümkündür.

Bu çalışmada saldırganlar tarafından sıklıkla kullanılan NTP ve DNS sunucularının yanı sıra 2018 senesinin Şubat ayından itibaren saldırganlar tarafından kullanılmaya başlanan ve günümüze kadar görülmüş en büyük hacimli saldırıların yaşanmasını sağlayan memcached sunucuları, ülkeler çapında keşfedildi ve keşfedilen bu sunucuların yükseltici olarak kullanılmalarına karşın sıkılaştırmalarının yapılıp yapılmamaları durumları araştırıldı. 43 Avrupa ülkesinde yapıldı. 43 ülkede yapılan bu çalışma neticesinde ülkeler arası sunucu yönetimlerinde sıkılaştırma bilincinin kıyaslama yapılabilmesinin yanı sıra bir saldırganın kısıtlı bir zaman içerisinde ne kadar saldırı kaynağı bulabileceği de tespit edildi. Elde edilen sonuçlar Estonya gibi bazı ülkelerde sıkılaştırma bilincinin çok yüksek olduğunu gösterirken bazı ülkelerde bunun tam tersinin olabildiğini gözler önüne sermiş oldu.

Anahtar Kelimeler: Yükseltme saldırısı, Dağıtık yansıtılmış hizmet engelleme saldırısı, NTP, DNS, Memcached

ABSTRACT

Master of Science

An Analysis of DRDoS Amplifiers in Turkey and Europe

Emre Murat ERCAN

TOBB University of Economics and Technology
Institute of Natural and Applied Sciences
Department of Computer Engineering
Information Security

Supervisor: Prof. Dr. Ali Aydın SELÇUK

Date: August 2018

Denial of Service attack continue from the past to the present by increasing their effectiveness with different strategies. Distributed Reflected Denial of Service (DRDoS), also known as Amplification Attack, is the new trend in the types of service blocking attacks. Attackers typically use services that use the UDP protocol as a reflector in Distributed Reflected Denial of Service attacks. The attacker's BotNets spoof the victim's IP address and send queries to UDP-based services. The responses generated by the reflectors go to the victim, allowing the victim's service to be temporarily disabled or delivered with very large delays. In order to increase the attack efficiency in these queries made by attackers, it is generally preferred to produce large amount of response data. NTP, DNS and memcached services are some of the protocols that generate high rate response data.

The power of attacks is directly proportional to the number of reflectors on the Internet. The ability to reduce attacks is indirectly in the hands of all UDP-based server administrators.

Hardening known weaknesses of servers will prevent them from being used as amplifiers or reflective in attacks. Although a number of compression methods have already been established for many services currently used during DRDoS attacks, it is possible to find a large number of reflectors on the Internet.

In this study, the NTP and DNS servers frequently used by attackers, as well as memcached servers, which have been used by attackers since February 2018 and which have led to the greatest volume of attacks to date, have been discovered throughout the countries, and the use of these servers as an amplifier has been investigated. Research has focused on 43 European countries. As a result of this study conducted in 43 countries, it was determined that the awareness of hardening in server administration between countries can be compared. The results show that in some countries, such as Estonia, the awareness of hardening is very high, and in some countries it has shown that the opposite can happen.

Keywords: Distributed reflected denial of service, Amplification attack, NTP, DNS, memcached

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım, bilgi ve birikimlerini benden esirgemeyen başta Ali Aydın SELÇUK olmak üzere, yüksek lisans öğrenimim ve çalışma hayatım boyunca her zaman yanımda olan Bahtiyar BİRCAN'a, öğrenim hayatım boyunca desteğini hiç esirgemeyen annem F. Güllü HAYDAR, babam Alican ERCAN' a, ve yol arkadaşım Esra ÇALIŞKAN' a, çalışmalarım sırasında her zaman yanımda hissettiğim; Çağan CEBE, Ahmet ATEŞ, Serkan AYDIN, Onur Şafak GÖRÜRÜM, Tülin DEMİRALP, Sertaç KATAL' a ve kıymetli tecrübelerinden faydalandığım TOBB Ekonomi ve Teknoloji Üniversitesi Bilgisayar Mühendisliği Bölümü öğretim üyelerine çok teşekkür ederim.

İÇİNDEKİLER

Sayfa

ŞEKİL LİSTESİ

Sayfa

ÇİZELGE LİSTESİ

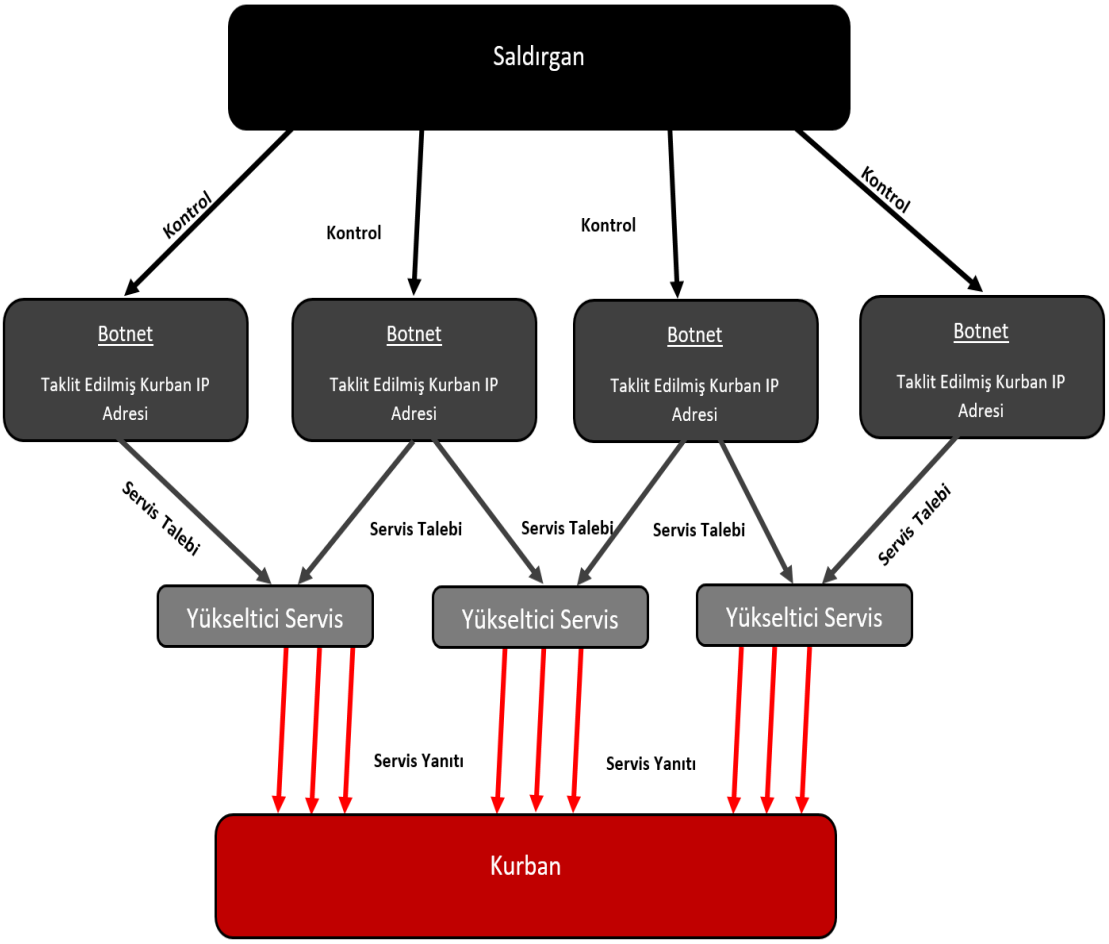
Sayfa

KISALTMALAR

DoS	: Denial of Service
DdoS	: Distributed Denial of Service
DRDoS	: Distributed Reflected Denial of Service
BAF	: Byte Amplification Factor
PAF	: Packet Amplification Factor
NTP	: Network Time Protocol
SNMP	: Simple Network Management Protocol
SSDP	: Simple Service Discovery Protocol
QOTD	: Quote of the Day
DNS	: Domain Name Service
P2P	: Peer to Peer
CVE	: Common Vulnerabilities and Exposures
CVSS	: Common Vulnerability Scoring System
IoT	: Internet of Things
CIDR	: Classless inter - domain routing

1. GİRİŞ

Bilinen en eski siber saldırılardan birisi olan hizmet engelleme saldırıları, internet kullanımının hayatımızın her alanına girmesi ile birlikte daha da sık karşılaşılır hale gelmiştir. Yıllar içerisinde saldırgan profillerinin değişmesinin yanı sıra saldırı metotları da alınan tedbirlerin üstesinden gelebilmek amacı ile geliştirilmiştir. Saldırılar; ticari servisler, politik siteler ve daha pek çok farklı servise yönelik olarak değişik motivasyonlarla yapılabilmektedir. Bir Dağıtık Hizmet Engelleme Saldırısında (DDoS), saldırganlar, hedef sunucunun bant genişliğini ya da hedefin sahip olduğu CPU ve bellek gibi diğer kaynaklarını tüketmeyi hedefler. Tüm bu saldırı faktörleri, hedefin hizmetlerini durdurabilmekte veya yavaşlatabilmektedir [1]. Dağıtık Yansıtılmış Hizmet Engelleme Saldırısı (DRDoS) diğer bir adı ile Yükseltici Saldırılarıları, genellikle doğrudan hedefin bant genişliğini tüketmeye yönelik olarak yapılmaktadır. 2012 senesinin sonundan itibaren etkinliğini göstermeye başlayan bu saldırı, klasik dağıtık hizmet engelleme saldırılarında olduğu gibi botnetler ile yapılmaktadır. Saldırının başarım mantığında iki temel husus vardır. Bu hususlardan birisi, saldırılar güçlerini yükseltici faktörlerinden almaktadır. DRDoS saldırılarında önemli bir diğer husus ise bu saldırılarda genel olarak UDP tabanlı protokollerin seçilmesidir. Bunun altında yatan temel sebep: UDP tabanlı protokollerin 3 lü el sıkışma olmaksızın işlemleri gerçekleştirmek olarak tanımlanan "güvenilmez" çalışma prensibidir. Bu prensip sayesinde saldırganlar, hedef aldıkları servisin IP adresini taklit ederek, yansıtıcılar tarafından oluşturulmuş cevapların, saldırılan sisteme gönderilmesini sağlarlar. Şekil 1.1'de dağıtık yansıtılmış hizmet engelleme saldırılarının çalışma modeli gösterilmiştir. Yapılan araştırmalara göre, TCP tabanlı protokoller kullanılarak da yükseltici saldırılarının yapılabileceğinin görülmesine karşın bu durum çalışmamızda kapsam dışı bırakılmıştır [2].



Şekil 1.1: Dağıtık yansıtılmış hizmet engelleme saldırısı çalışma modeli.

Saldırganlar, dağıtık yansıtılmış hizmet engelleme saldırıları sırasında, yansıtıcılar olarak büyük yükseltici faktörüne sahip servis sorgularını seçmeye özen göstermektedir. Bazı protokollerde elli bin katına kadar çıkabilen bu büyük faktörler sayesinde saldırganlar, yapılan küçük sorgulara gelecek olan cevapların çok büyük hacimli olmasını sağlarlar. Bu da en düşük efor en yüksek güç anlamına gelmektedir. Yükseltici faktörü, sunucuların versiyonuna, sıkılaştırma yöntemlerine ve protokolün kendisine göre değişebilmektedir. Gerek geçmişte yapılan çalışmalar gerekse hali hazırda yaşanmış ve yaşanmakta olan dağıtık yansıtılmış hizmet engelleme saldırıları, NTP, DNS ve memcached servislerinin hizmet sağlayıcılarda büyük problemler yaratabileceklerini gözler önüne sermiştir.

Yükseltici faktörleri iki farklı şekilde ele alınmaktadır. Bunlardan biri, paket yükseltici faktörüdür (PAF). Paket yükseltici faktörü; cevap olarak sisteme dönüş yapan paket sayısının, yapılan sorgu için gönderilen paket sayısına oranlanması ile elde edilmektedir. Paket yükseltme faktör denklemi Eşitlik 1.1'de gösterildiği gibidir.

$$Paket\ Yükseltme\ Faktörü = \frac{Sisteme\ Dönüş\ Yapan\ Paket\ Sayısı}{Sorgu\ İçin\ Gönderilen\ Paket\ Sayısı} \quad (1.1)$$

Diğer bir yükseltici faktörü ise byte yükseltici faktörü olarak tanımlanmaktadır (BAF) [3]. Cevap olarak sisteme dönüş yapan verinin byte olarak büyüklüğünün, gönderilen sorgunun büyüklüğüne oranlanması ile elde edilir ve elde edilen bu oran dağıtık yansıtılmış hizmet engelleme saldırıları için daha kritik durumdadır. Bunun temel nedeni yapılan araştırmalara göre; paket yükseltici faktörü, tespit edilebilen en kötü senaryolar için 10,6x iken memcached servisi için byte yükseltici faktörü 50000x üzerine çıkabilmektedir. TCP tabanlı protokoller üzerine yapılmış çalışmalarda en yüksek byte yükseltici faktörü TELNET protokolü için tespit edilmiştir [4]. 79,625x olarak tespit edilen bu oran UDP tabanlı protokollere kıyasla çok daha düşük kalmaktadır. Byte yükseltme faktör denklemi Eşitlik 1.2'de gösterildiği gibidir.

$$\text{Byte Yükseltme Faktörü} = \frac{Sisteme\ Dönüş\ Yapan\ Byte\ Miktarı}{Sorgu\ İçin\ Gönderilen\ Byte\ Miktarı} \quad (1.2)$$

Dağıtık yansıtılmış hizmet engelleme saldırılarında yansıtıcı olarak sıklıkla kullanılan servislerden bir tanesi DNS'tir. TCP ve UDP protokollerinin her ikisini de destekleyen bu protokol, port 53 üzerinde çalışmaktadır ve tekbiçimli kaynak konumlayıcıların (URL) veya tam etki alanı adlarının (FQDN) IP adreslerine çözümlenmesini sağlamak amacı ile kullanılmaktadır.

Bu sistemin saldırganlar tarafından kullanılmasının üç temel nedeni vardır. Sıkılaştırmaların yapılmadığı DNS sunucularında büyük ölçekli yükseltici faktörü mevcuttur ve internette birçok servis ile karşılaştırıldığı zaman sayısal olarak çok fazla DNS sunucusu görülmektedir.

DNS sunucularının yaygın bir şekilde kullanılmasındaki diğer bir neden ise gerçek sorgular ile saldırı sorgularının ayırt edilmesinin güçlüğüdür.

Dağıtık yansıtılmış hizmet engelleme saldırıları sırasında yansıtıcı olarak yaygın bir şekilde kullanılan bir diğer protokol ise NTP protokolüdür. Düzgün bir şekilde sıkılaştırmamış NTP sunucusunun yükseltici faktörünün çok yüksek seviyelere çıkması, saldırganlar için büyük avantaj sağlamaktadır. Günümüze kadar gerçekleştirilmiş büyük hacimli saldırılarda, üzerinde NTP servisi çalıştıran yansıtıcıların kullanımı sıklıkla gözlemlenmiştir. İnternet ya da intranet üzerinde haberleşen cihazların zaman senkronizasyonunu sağlamak amacı ile kullanılan bu protokol UDP port 123 üzerinde çalışmaktadır. Bağlantılar NTP sunucuları arasında olabileceği gibi NTP sunucusu ile haberleşen diğer cihazlar arasında da gerçekleşebilmektedir. Zaman senkronizasyonunun düzgün bir biçimde sağlanması, güvenlik sağlayıcı sistemler açısından kritik bir önem arz etmektedir. Günümüzün olmazsa olmaz güvenlik teknolojilerinden "Güvenlik Olay ve İhlal Yönetimi (SIEM)" cihazının başarısı, birbirleri ile etkileşim halinde olan cihazların etkin zaman senkronizasyonuna bağımlıdır [5].

Saldırılar için bir diğer önemli kaynak ise memcached sunucularıdır. UDP ve TCP port 11211 üzerinde çalışabilen bu servis, saldırganlar için kullanılabilirliğini Şubat 2018 tarihinden itibaren göstermektedir. Asıl amacı dinamik web uygulamalarının yüklenme sürelerini en aza indirmek olan bu servis, 50000x yükseltici faktörü ile bilinen en yüksek çoklayıcı faktörüne sahiptir. 2018 senesinin Şubat ayında memcached sunucuları kullanılarak günümüze kadar gerçekleştirilmiş olan en yüksek hacimli hizmet engelleme saldırıları sırasıyla 1,3 Tb/s ve 1,7 Tb/s olarak gerçekleştirilmiştir.

1.1 Tezin Amacı

Günümüzde servislerin erişilebilirlik ihtiyaçlarının artması ile birlikte hizmet engelleme saldırıları, saldırganlar için daha da önemli bir silah haline gelmiştir. UDP tabanlı dağıtık yansıtılmış hizmet engelleme saldırıları karşısında saldırılan tarafların alabileceği tedbirler mevcuttur. Kurban tarafından alınacak doğru tedbirler ile bu saldırıları genellikle etkisiz hale getirebilmek mümkündür. Ancak bu tedbirler mali kaynak gerektirmektedir.

Bu tedbirler saldırı gücünü engelleyebilmelerine karşın, yansıtıcı olarak kullanılabilecek sistemlerin sıkılaştırılmış olması da saldırganların gücünü önemli derecede azaltacaktır.

Bu çalışmada saldırganlar tarafından sıklıkla kullanılan DNS, NTP ve memcached sunucularının Almanya, Andorra, Arnavutluk, Avusturya, Belarus, Belçika, Birleşik Krallık, Bosna Hersek, Bulgaristan, Çekya, Danimarka, Ermenistan, Estonya, Finlandiya, Fransa, Hırvatistan, Hollanda, İrlanda, İspanya, İsveç, İsviçre, İtalya, İzlanda, Karadağ, Kuzey Makedonya, Letonya, Lihtenştayn, Litvanya, Lüksemburg, Macaristan, Malta, Moldova, Norveç, Polonya, Portekiz, Romanya, Rusya, Sırbistan, Slovakya, Slovenya, Türkiye, Ukrayna ve Yunanistan kapsamında tespitleri gerçekleştirildi.. Tespit işlemlerinin tamamlanması sonrasında hazır araçlar kullanarak gerek ise yazılan kod parçacıkları ile yükseltici olarak kullanıma engel olacak tedbirlerin alınması durumları derinlemesine araştırıldı. Küresel sıkılaştırma bilincinin ortaya konulmasına ek olarak, tespit edilip yayınlanan tüm sıkılaştırma yöntemlerine karşın, saldırganların hali hazırda güçlü saldırıları gerçekleştirebilecekleri kadar yükselticiyi rahat bir şekilde keşfedebilecekleri tespit edildi.

1.2 Literatür Araştırması

UDP tabanlı dağıtık yansıtılmış hizmet engelleme saldırılarının en temel gereksinimlerinden bir tanesi IP adreslerinde yapılan taklit etmelerdir. Konu ile ilgili bilinen ilk çalışmalardan olan, 1989 senesinde yayınlanmış ve TCP/IP protokolünde gerçekleşebilecek saldırıları ele alan çalışmadır.

Bu çalışmada ICMP paketleri ile hizmet engelleme saldırıları, yanlış konfigüre edilmiş DNS sunucularından kaynaklanan hizmet durmaları, çok sayıda yayın gönderilmesinden kaynaklanan hizmet engelleme saldırıları gibi konuların yanı sıra, IP adresleri taklit edilerek hizmet engelleme saldırılarının gerçekleşebileceği de ele alınmıştır [6].

2014 senesinde kadar yayınlanmış makaleler incelendiğinde, genellikle dağıtık hizmet engelleme saldırılarının tespit edilmesi, filtrelenmesi veya izlenmesi üzerine yoğunlaşılmış çalışmalar olduğu görülmektedir.

2014 senesinde Rossow ve çalışma ekibi bir dizi önemli araştırmalar yapmaya başlamıştır.

Bu çalışmalardan ilki, byte yükseltici faktörü, paket yükseltici faktörü gibi önem arz eden tanımların yapıldığı ve iki kapalı sistemi izleyerek bir çok UDP tabanlı servisler için bu değerlerin tespit edildiği çalışmadır [3]. Bu çalışmanın devamı ve detaylandırılması niteliğinde olan ikinci çalışma da yine aynı ekip içerisinde yer alan Marc Kührer öncülüğünde gerçekleşmiştir. USENIX 2014'de çıkan bu çalışmada DNS ve NTP gibi bazı kritik servisler için işletim sistemi detayında çalışmaların gerçekleştirilmesinin yanı sıra NTP sunucuları, örnek çalışma olarak seçilmiş ve zaman içerisinde yükseltici sayıları ve oranlarındaki düşüş gösterilmiştir. Ayrıca bu makale içerisinde TCP tabanlı protokollerin de 79 kata kadar yükseltici faktörüne sahip olabileceği belirtilmiştir [2].

Yine aynı senenin Ağustos ayında çıkan Kührer ve çalışma ekibinin bir diğer makalesinde ise bu sefer 13 farklı TCP protokolü ele alınmış olup ve bu protokollerde birden çok parametre denemesi ile TCP tabanlı bu protokollerin byte yükseltici faktörleri tespit edilmiştir [5].

1.3 Yaşanmış Olaylar

Tüm bu çalışmaların yanı sıra günümüze kadar Türkiye de dâhil olmak üzere dünyanın çeşitli ülkelerinde etkileri çok büyük olmuş birçok dağıtık yansıtılmış hizmet engelleme saldırısı gözlemlenmiştir.

Tüm bu çalışmalar ve yaşanan olaylar, hali hazırda sıkılaştırma zorluğu orta-alt seviye olan yükselticilerin tespit edilmesi ihtiyacını doğurmuştur

Verilen hizmetlerin erişilebilirlik ihtiyaçlarının artması ile birlikte UDP tabanlı protokollerin kullanımı artmıştır. Bu artışın doğal sonucu olarak dağıtık yansıtılmış yükseltme saldırılarında kullanılmak üzere internette keşfedilebilen yükseltici sayısı da artmıştır. Yükseltici saldırısı olarak tanımlanan, bilinen ilk büyük saldırılar 2012 senesinde gerçekleştirilmeye başlanmıştır. Saldırıların etkinliğini arttırdığı görülen 2012 senesinden itibaren yapılmış olan çalışmalarda; NTP, SNMP, SSDP, NetBIOS gibi hali hazırda kullanılan UDP tabanlı protokollerin yanı sıra CharGEN, QOTD gibi güncel hayatta sıklıkla karşımıza çıkmayan eski servislerin, BitTorrent, Kad gibi Peer to Peer (P2P) dosya paylaşım servislerinin ve Queke 3, Steam gibi oyun sunucularının yükseltici faktörleri ele alınmış ve bu servislerin saldırganlar tarafından kullanılabileceği gözler önüne serilmiştir [7].

Prolexic tarafından yayınlanmış olan rapora göre, 2013 senesinin Mayıs ayında zamanının en yüksek hacimli dağıtık yansıtılmış hizmet engelleme saldırısı DNS sunucularının yükseltici olarak kullanılması ile gerçekleştirilmiştir. Gerçek zamanlı finansal platforma yapılan bu saldırı 167 Gb/s'lik hacme ulaşmıştır [8]. Bu saldırının yanı sıra 2013 senesinde en az 100 Gb/s hacim sağlamayı başaran 3 saldırı daha gerçekleştirilmiştir. Bu saldırılardan iki tanesinin DNS sunucuları ile gerçekleştirildiği bilinmektedir [9].

Ağustos 2013 tarihinde gerçekleştirilen bir yükseltme saldırısında saldırganlar GreenNet şirketini hedef aldılar. Sunucu barındırma hizmeti veren bu şirketin o dönem hizmet verdiği kurumlar arasında Zimbabve İnsan Hakları Forumu vardı [10].

2013 senesinden DNS sunucuları ile gerçekleştirilen bir diğer saldırı ise Spamhaus sistemlerine gerçekleştirildi. 2013 Mart ayında gerçekleştirilen bu saldırıda DNS yükselticilerinin kullanılmasının yanı sıra "SYN flood" saldırısı da eş zamanlı olarak yapıldı ve saldırganlar yer yer 300 Gb/s'lik hacim elde etmiş oldular. Spamhaus'un anti spam amacı ile internette hizmet verdiği sunucular, bu saldırının sonucu olarak kısa bir süre için servis veremedi [11,12].

2013 senesinde göze çarpan bir diğer saldırı ise NTP sunucularının yansıtıcı olarak kullanılması ile gerçekleştirildi. Bu saldırı yaklaşık olarak 100 Gb/s hacme erişirken Dota2 ve Leage of Legands gibi küresel olarak on binlerce kişinin oynadığı oyun sunucularının servis dışı kalmasına sebep oldu [9, 13].

Günümüzde en çok karşılaşılan yükseltici saldırılarını incelediğimiz zaman bunların başında DNS sunucularının yükseltici olarak kullanıldığı saldırılar olduğu görülmektedir. İnternet üzerinde çok sık bulunmasının yanı sıra sıkılaştırma işlemleri sadece ele alınacak NTP ve memcached sistemleri gibi yalnızca güncellemeleri yapılarak ilgili sıkılaştırmaların gerçekleşebilmelerine olanak vermeyecektir. Ayrıca hatırı sayılır yükseltici faktörüne sahip olan DNS sunucuları için yükseltici faktörü iki farklı biçimde ele alınabilmektedir. İnternete açık ancak yetkili olmayan çözümleyiciler için paket yükseltici faktörü 1,32x iken byte yükseltici faktörü en kötü %10'luk dilim için 64,1x, en kötü %50'lik dilim için 61,2x'dir. Yetkili çözümleyicilerde ise yükseltici faktör oranları biraz daha yüksektir.

Bu sunuculardaki ortalama paket yükseltici oranı 2,08x iken en yüksek faktörlü %10'luk sunucu dilimi için byte yükseltici faktörü 98,3x faktör, en kötü %50'lik dilim için 76,7x faktördür [3]. Bu faktörler alan hakkında elde olan tüm verilerin çekilebilmesini sağlayan "ANY" sorgusu ile sağlanabilmektedir. Bu isteğin yanıtı olarak, sorgu yapılan sunucu istek yapan cihaza sorgulanan etki alanı ile ilgili kayıtlı olan tüm bilgileri gönderir. Bu bilgiler özyinelemeli sorgular ile birleşince saldırganlar tarafından kullanılabilir bir durum oluşturmaktadır. Bu açıklıklar Ulusal Zafiyet Veri tabanı (NVD) içerisinde de tanımlanmış, tekil tanımlayıcıları verilmiş ve otomatize edilmiş protokol tarafından etki değerleri puanlanmıştır.

Ele alınan zafiyetlerin "Bilinen Tehditlerin Skorlanması Sistemi" (CVSS) ölçütlerine göre puanlanması Çizelge 2.1'de gösterilmiştir. DNS sunucularının özyinelemeli sorgulara cevap vermesi ISC BIND sunucu sistemleri için CVE-2006-0987 olarak tanımlanmış ve temel etki skoru CVSS v2.0'a göre 5.00 - orta düzey olarak hesaplanmıştır [14].

Windows Server 2003, Windows 2000 ve Microsoft Windows NT 4.0 üzerinde çalışan DNS sunucu sistemi için varsayılanda özyinelemeli sorgu yapılabilmesi CVE-2006-0988 olarak tanımlanmıştır. Bu zafiyetin temel etki skoru CVSS v2.0'a göre 7.8 - yüksek olarak ele alınmıştır [15].

İlgili sıkılaştırma yayınlarının çok eski tarihlere uzanmasına karşın internet ortamında özyinelemeli sorguya açık olan birçok sunucu bulunmaktadır. Bu sunucular ile yapılmış, büyük yankılar yaratan birçok saldırı gerçekleştirilmiştir.

Bu saldırılardan bir tanesi ".tr" uzantılı alan adlarının yönetilmesini sağlayan "nic.tr" sunucularına yapılmıştır. 2015 senesinin Aralık aydında düzenlenen bu saldırı özel bir hedef gözetmeksizin tüm ülke internetini belirli ölçülerde yavaşlatmıştır. Yaşandığı tarih itibari ile en büyük saldırılardan birisi olarak kayda geçen bu olay hızlı aksiyonlar ile bertaraf edilmiştir. "Nic.tr" yetkilileri tarafından yapılan açıklamaya göre saldırılar, yer yer 200 Gb/s'nin üzerinde bir hacim üretmiştir [16].

Bu saldırıdan yaklaşık bir yıl sonra, 2016 senesinin Ekim ayında saldırganlar tarafından aynı yöntemler ile küresel bir hedefe saldırı gerçekleştirdi. Saldırının hedefinde bu sefer "Dyn" şirketi vardı. Bu şirket uluslararası birçok firmaya ve devlet kurumlarına dinamik DNS hizmeti vermekteydi.

Müşterileri arasında Airbnb, Amazon.com, BBC, CNN, The Boston Globe, Fox News, The Guardian, GitHub, HBO, Netflix The New York Times, PayPal, Pixlr, PlayStation Network, Pinterest, Quora, Reddit, SoundCloud, Spotify, Starbucks, Tumblr, Twitter, Verizon Communications, Visa, The Wall Street Journals, Xbox Live gibi dünyaca ünlü şirketler bulunmaktaydı. Dyn saldırısı sırasında bu platformların çoğunda önemli erişim problemleri yaşandı [17].

Bu şirketlerin yanı sıra saldırı sırasında İsveç Hükümeti internet sitesi ve İsveç Sivil Acil Durum Dairesi 'de erişim problemleri ile yüz yüze geldi. Dyn saldırısının önemli bir boyutu ise bu saldırıda botnetlerin "Mirai" zararlı yazılımı ile ele geçirilmiş olan nesnelerin interneti (IoT) cihazlarından oluşmasıdır. Bu durum, gelecekte nesnelerin interneti ürünlerinin yaşatabilecekleri problemleri ele almak açısından önem arz etmektedir. IoT cihazlarının gündelik hayatımızın bir parçası haline gelmesi ile saldırganların çok daha güçlü saldırıları gerçekleştirebilmeleri olasıdır.

Saldırganların yükseltici olarak sıklıkla kullandığı bir diğer servis ise NTP'dir. NTP sunucularının yansıtıcı olarak kullanılmasındaki temel sebep, güçlü paket ve byte yükseltici faktörüdür. Zaman senkronizasyonunun tutarlı bir şekilde yapılması için kullanılan bu protokolde paket yükseltme faktörü ortalama 10,61x byte yükseltici faktörü en kötü %10'luk dilim için 4670x, en kötü %50 için 1083x'dir [3].

Bu faktörlerin oluşması "monlist" sorgusunun işlevselliğinin sıkılaştırılması ile alakalıdır. Saldırgan bu sorgu sayesinde oldukça büyük BAF ve PAF oranları elde edebilmektedir. Yönetimsel amaçlar için tasarlanmış bu sorguya cevap olarak sorgu yapılan sunucuya bağlanmış olan son 600 hizmet alan cihazların bilgileri döner. Bu bilgilerin içerisinde, sisteme bağlanan kişilerin IP adresleri, hali hazırda kaç defa bağlandıkları, kullandıkları, sunucunun versiyonu gibi ayrıntılı bilgiler mevcuttur. Eğer bir sıkılaştırma yapılmamış ise bu sorgu herkes tarafından yapılabilir.

Monlist sorgularının herkes tarafından yapılabilmesi ile DRDoS saldırılarının meydana gelmesi CVE-2013-5211 olarak tanımlanmış ve temel etki skoru CVSS v2.0'a göre 5.0 - orta olarak hesaplanmıştır [18].

2013 senesinden itibaren NTP sunucularının yansıtıcı olarak kullanılma durumu ortaya çıkmıştır. NTP sunucularının yükseltici olarak kullanıldığı en etkili saldırılardan bir tanesi 2014 senesinde gerçekleştirilmiştir.

Cloudflare tarafından yapılmış açıklamada Şubat 2014'te bir müşterilerinin 400 Gb/s'lik bir saldırı ile karşı karşıya kaldıklarını belirtilmişlerdir. Bu açıklamada, saldırganların 1,298 farklı ağdan 4,529 farklı NTP sunucusunu aracılığı ile saldırıyı gerçekleştirdiklerini ve her bir yansıtıcının yaklaşık olarak 87 Mb/s'lik trafik oluşturduğu belirtilmiştir [19].

Memcached, dinamik uygulamaları için tasarlanmış olup, anahtar - değer eşlemesi ile uygulamaların performansını arttırmaya yönelik bir servistir [20]. Günümüzde, dağıtık yansıtılmış hizmet engelleme saldırıları için en yeni trend bu servistir. Şubat 2018'in son gününde saldırganların GitHub sistemlerine yaptığı DRDoS saldırısı ile zafiyet ortaya çıkmıştır. Öncesinde literatürde konu ile ilgili bir çalışma yoktur. Saldırı sonrasında yapılan değerlendirmeler neticesinde yükseltici faktörünün 50000x'e kadar çıkabileceği tespit edilmiştir. Sistemin çalışma prensibi gereği yükseltici faktörünü düşürebilecek bir metot yoktur.

Buna karşın memcached sunusunun internete açık olma gereksiniminin iyice incelenmesi, şayet internet üzerinden servis vermesi gerekiyor ise UDP port 11211 üzerinde çalışmasının durdurulması gereklidir. İnternete açık ve UDP üzerinden işlem yapılarak memcached sunucuları aracılığı ile saldırıların düzenlenebilmesi CVE-2018-1000115 olarak tanımlanmış ve temel etki skoru CVSS v3.0 a göre 7.0 - yüksek CVSS v2.0 göre 5.0 - orta olarak ele alınmıştır [21].

GitHub saldırısı sırasında, saldırganların oluşturduğu hacim ilk defa Tb/s sınırını aşmıştır. GitHub yetkilileri tarafından yapılan açıklamaya göre saldırı kaynağı binlerce farklı otonom sistemdir. Saldırının ilk fazı 17:21'de gerçekleştirilmiştir ve bu fazda 1,35 Tb/s hacim oluşmuştur. Bu hacmin oluştuğu esnada saldırganlar tarafından saniyede 126,9 milyon paket gönderildiği gözlemlenmiştir [22]. Savunma sisteminin başarı ile devreye girmesi sonucunda GitHub sistemi 13 dakika içerisinde normal seviyelere dönmüştür. Saldırının ikinci fazı 18:30 sularında gerçekleştirilmiş ve bu fazda yaklaşık olarak 400 Gb/s'lik hacim gözlemlenmiştir. GitHub saldırısından bir kaç gün sonra hacim rekoru tekrar memcached sunucularının yansıtıcı olarak kullanılması ile kırılmıştır. Netscout'un yaptığı açıklamada saldırı ile ilgili detaylara yer verilmez iken saldırının Amerika'da bulunan bir servis sağlayıcıya düzenlendiği, memcached sunucularının yükseltici olarak kullanıldığı ve saldırı sırasında 1,7 Tb/s hacminin gözlemlendiği doğrulanmıştır [23].

Çizelge 2.1 : DNS, NTP ve memcached açıklıkları ve standart etki değerleri.

Protokol	CVE Kodu	CSS v2.0 Skor			CSS v3.0 Skor		
		Temel Skor	Etki Skoru	Sömürülme Kolaylığı	Temel Skor	Etki Skoru	Sömürülme Kolaylığı
DNS	2006-0987	5.0	2.9	10.0	-	-	-
DNS	2006-0988	7.8	6.9	10.0	-	-	-
NTP	2013-5211	5.0	2.9	10.0	-	-	-
Memcached	2018-1000115	5.0	2.9	10.0	7.5	3.6	3.9

Çizelge 2.1'de tüm çalışmalar için CVSS versiyon 2 puanlandırması mevcut iken sadece memcached sunucuları için yapılan değerlendirmede versiyon 3 puanlaması bulunmaktadır. Her iki versiyon için, tüm puanlar 0 ile 10 arasında hesaplanmaktadır.

Algoritmaya girilmiş olan değerler ile temel skor elde edilirken etki skoru saldırı sonrasında gizlilik, bütünlük ve erişilebilirlik etkilerini ele alır.

Sömürülme kolaylığı ise saldırganın ağ ile olan ilişkisini almaktadır. Versiyon üç için sömürülme kolaylığında kullanıcı erişimi parametreleri, etki skoru için değişkenlik durumları ve sistem ihtiyaçları da eklenmiştir. İki sürüm için de çevrim içi hesaplama yapabilmek mümkündür [24,25].

2. METODOLOJİ

Bu çalışmada dağıtık yansıtılmış hizmet engelleme saldırılarında kullanabilecek UDP tabanlı servislerden üç odaklanıldı. Odak noktaları araştırma sırasına göre DNS, NTP ve memcached sunucularından oluştu. Çalışmalar 43 ülke ile sınırlandırıldı. Bu ülkeler arasında Almanya, Büyük Britanya, Fransa, İspanya, Rusya gibi çok büyük nüfuslu ülkelerin yanı sıra Estonya gibi küçük ancak yaşadıkları olaylar sebebi ile güçlü tedbirler almak konusunda nam salmış ülkeler de seçildi. Çalışmanın ilk kritik adımı kullanılacak ülke IP CIDR'larını belirlemekti. Bu konu ile ilgili çok çeşitli kaynak olmasına karşın, güncel veri tabanına ulaşmak kritik önem arz etmekteydi. İsterleri en iyi şekilde karşılayacak, güncel veri tabanının Ivan Erben tarafından yazılmış olan kod parçacığı ile internet üzerinde günlük olarak bu listelerin çekildiği veri tabanı olarak seçildi [26,27]. Yapılan çalışmalar esnasında DNS çalışmaları için Ocak ve Şubat 2019 tarihlerinde çekilmiş olan veri tabanları kullanılırken NTP ve memcached çalışmalarında Mart 2019 tarihinde çekilmiş olan veri tabanları kullanılmıştır.

Kullanılacak veri tabanı belirlendikten sonra söz konusu 43 ülke için varsayılan portlarından yayın yapan DNS, NTP ve memcached sunucularının internet üzerinden keşfedilmesi problemi ele alındı. Bu denli geniş kapsamı olan bir çalışma için elde çok az sayıda alternatif olduğu görüldü. Bu alternatifler arasından gerek referans alınan çalışmalarda kullanılmış olan gerek 2017 senesinden itibaren gerçekleştirilen çalışmalarda kullanılmış "zmap" tarama aracı tercih edildi [28].

Tercih nedeni olarak, Ağustos 2013'te USENIX güvenlik sempozyumunda tanıtılmış olan bu açık kodlu tarama aracı, doğru şartlar sağlandığı durumlarda bütün IPv4 adreslerini 5 dakikada tarayabileceği iddiasında olmasıdır.

İçerisinde çok farklı tarama modülleri barındıran bu araç; 1 gigabitlik bağlantısı olan bir bilgisayarın ele alındığı daha olası senaryolar için bütün IPv4 adreslerini yaklaşık olarak 45 dakika içerisinde tarayabilmektedir [29].

Çizelge 3.1'de ülke genelinde açık sunucuları tespit edilmesi amacı ile yapılan port taramalarının yaklaşık olarak tamamlandığı süreler dakika cinsinden verilmiştir. Geçmiş çalışmalarımızdan gelen tecrübelere dayanarak, tarama işlemleri ilk olarak DNS sunucuları için gerçekleştirilmiştir [30, 31]. Zmap aracı içerisinde DNS sorgusunun yapılabilmesi için üç farklı özelleştirilmiş sorgu metodu vardır. Metotlar zmap aracı içerisindeki özelleştirilmiş paketler ile gerçekleştirilir. Bu metotlardan dns_53_queryAwww.google.com.pkt metodu sorgu yapılan sunucudan google.com alanı için "A" kayıtlarını sorgularken dns_53_ queryAwww.google.it.pkt sorgusu ile aynı işlem google.it alanı için yapılır. Üçüncü sorgu yöntemi olan dns_53.pkt metodunda ise bağlanmış TXT kayıtları üzerinden DNS dağıtıcıları ve versiyonları sorgulanır. Tüm bu metotlar UDP taramaları ve TCP taramaları ile gerçekleştirilebilir [32]. Ayrıca herhangi özel bir sorgu kullanılmayarak sadece port 53 üzerinden yayın yapılıp yapılmama durumu da sorgulanabilir. Bu da sonuç olarak sekiz farklı tarama metoduna sahip olunduğu anlamına gelmektedir. Herhangi bir özel metot kullanılmadan, sadece UDP port 53 taramasının yapılması durumunda; verimli bir sonuç elde edilebilmesi beklentisine karşın, UDP tabanlı taramalar gerçekleştirildiğinde, birbirini içeren farklı IP kümelerinin sonuç olarak döndüğü görülmüştür. Bu sebepten ötürü taramalar sonuçlar sabitlenene kadar gerçekleştirilmiştir. Yapılan çalışmalar neticesinde; TCP tabanlı dns_53_queryAwww.google.com.pkt sorgu kullanımı, UDP tabanlı dns_53_ queryAwww.google.it.pkt sorgu kullanımı ve UDP tabanlı özel sorgu olmaksızın gerçekleştirilen standart sorgulamalar altışar defa tekrarlandığı durumda, sonuçların sabitlendiği tespit edilmiştir. DNS taramaları esnasında, ülkeler özelinde kullanılmış zmap tarama komutunun genelleştirilmiş hali Ek 1'de verilmiştir.

.

Çizelge 3.1: Protokol özelinde ülkelerin zmap ile dakika cinsinden yaklaşık taranma süreleri.

Ülke Adı	DNS	NTP	Memcached
Almanya	1652	92	92
Andorra	1	5	5
Arnavutluk	14	1	1
Avusturya	161	9	9
Belarus	43	2	2
Belçika	378	21	21
Birleşik Krallık	1656	92	92
Bosna Hersek	16	2	2
Bulgaristan	64	5	5
Çekya	132	7	7
Danimarka	174	10	10
Ermenistan	18	1	1
Estonya	23	1	1
Finlandiya	180	10	10
Fransa	1134	63	63
Hırvatistan	34	2	2
Hollanda	630	35	35
İrlanda	94	5	5
İspanya	414	23	23
İsveç	414	23	23
İsviçre	270	15	15
İtalya	672	42	42
İzlanda	17	1	1
Karadağ	12	1	1
Kuzey Makedonya	14	1	1
Letonya	29	2	2
Lihtenştayn	5	1	1
Litvanya	38	2	2
Lüksemburg	24	1	1
Macaristan	86	5	5
Malta	14	1	1
Moldova	24	1	1
Norveç	216	12	12
Polonya	288	16	16
Portekiz	95	5	5
Romanya	117	6	6
Rusya	630	35	35
Sırbistan	36	2	2
Slovakya	41	2	2
Slovenya	40	2	2
Türkiye	216	12	12
Ukrayna	159	9	9
Yunanistan	83	5	5

Zmap ile tarama işlemi tamamlandıktan sonra başka bir problem kendini göstermiştir. Ülke veri tabanının girdi olarak verilmesine karşın, taramaların çıktılarında birçok farklı ülkeden IP adresleri olduğu tespit edilmiştir. Zmap aracının geliştiricileri, hali hazırda UDP tabanlı taramaların değişkenlik gösterebileceğini, gelen yanıtların takip edilmesi gereksinimini belirttiği için bu durum doğal olarak karşılanmıştır. Bu problem, zmap çıktıları ile hali hazırda o ülke için kullanılan IP veri tabanını birleştirip, birden çok tekrar eden IP adreslerinin üzerinde port 53 çalışan bir cihaz olduğunu kabul ederek aşılmıştır.

Sunucuların keşif aşaması tamamlandıktan sonra bu cihazların açıklık kontrolünü yapma aşaması başlatılmıştır. İstenilen sonuçları detaylı olarak verebilecek bir çözüm bulunmadığı için bir kod parçacığı yazılmıştır. Bu kod parçacığının içerisinde "nslookup" komutu ile özyinelemeli sorgu yapılmıştır ve saldırganların temel olarak kullandığı "ANY" sorgusuna sunucuların cevap vermesi istenmiştir. Kod parçacığının genelleştirilmiş hali Ek 2'de gösterilmiştir. Gelen sonuçlar detaylı bir şekilde incelenmiş, dağıtık yansıtılmış hizmet engelleme saldırılarında yükseltici olarak kullanılabilecek sunucular tespit edilmiştir.

DNS çalışmalarının tamamlanması sonrasında çalışmanın ikinci aşaması olan NTP sunucularının tespiti ve incelenmesine başlanmıştır.

NTP sunucularının ülkeler çapında keşfedilmesi için tekrar zmap aracına başvurulmuştur. Bu araştırma sırasında aracın içerisinde olan NTP için hazırlanmış otomatik modül kullanılmıştır. Bu modül için yapılan araştırmalar neticesinde tek bir tarama ile yüksek verim elde edildiği tespit edilmiştir. NTP taramaları esnasında, ülkeler özelinde kullanılmış zmap tarama komutunun genelleştirilmiş hali Ek 3'de verilmiştir.

Üzerinde 123 portunu çalıştıran sunucular tespit edildikten sonra bu sunucuların dağıtık yansıtılmış hizmet engelleme saldırılarında yükseltici olarak kullanılabilme durumu incelenmiştir. Bu inceleme için "nmap" aracı kullanılmıştır [33]. Küresel olarak bilinirliği çok yüksek olan bu açık kaynaklı tarama aracı, dar kapsamlı ağ taramaları için kullanılmaktadır. Ağ içerisinde servis bilgilerinin tespit edilmesi, zafiyetli cihazların tespit edilmesi gibi birçok fonksiyona sahip bu araç, NTP sunucuları için de otomatik olarak "monlist" sorgusu sorabilme kabiliyetine sahiptir.

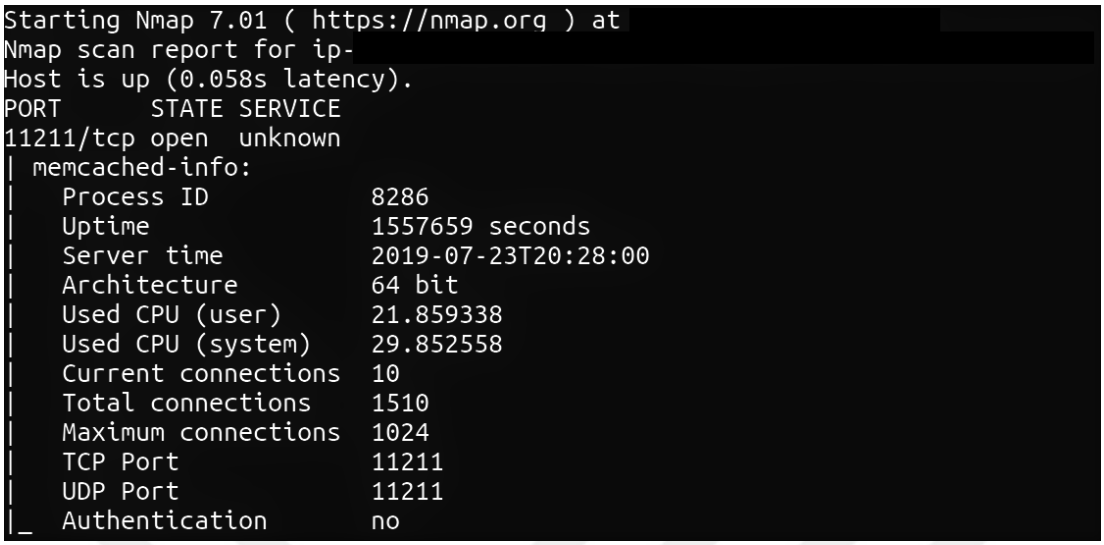
Bu kabiliyeti sayesinde belirlenen sunucular hızlı bir şekilde monlist sorgusuna tabi tutulmuştur. Nmap kullanılarak gerçekleştirilen “monlist” komutunun genelleştirilmiş hali Ek 4’te verilmiştir. Sunucuların bu sorguya verdiği yanıtlar detaylı olarak incelenerek saldırılarda yükseltici olarak kullanılabilme potansiyelleri tespit edilmiştir.

Bu çalışmadaki üçüncü ve son hedef olan IPv4 adresleri ile internet üzerinden yayın yapan memcached sunucularının tespit edilmesi ve dağıtık yansıtılmış hizmet engelleme saldırıları için yükseltici olarak kullanılabilme potansiyellerinin belirlenmesidir. Bu amaç ile tekrar zmap aracı ile taramalar gerçekleştirilmiştir. Memcached sunucularının gerek TCP gerek UDP protokolleri ile yayın yapabilmelerine karşın bu taramalarda TCP port 11211 üzerinden yayın yapan sunucuların keşfi gerçekleştirilmiştir. Bunun temel sebebi sıkılaştırma yapılmış sunucuların sadece TCP port 11211 üzerinden yayın yapabiliyor olmasına rağmen sadece UDP port 11211 üzerinden yayın yapan sunucuların olmaması beklentisidir. Memcached taramaları esnasında, ülkeler özelinde kullanılmış zmap tarama komutunun genelleştirilmiş hali Ek 5’te verilmiştir

İnternet üzerinden yayın yapan memcached sunucuları tespit edildikten sonra bu sunucuların UDP port 11211’den yayın yapma durumlarını tespit etme amacı ile nmap aracı kullanılmıştır. Nmap kullanılarak gerçekleştirilen ve memcached sunucuları ile ilgili detaylı bilgileri elde etmemizi sağlayan komutun genelleştirilmiş hali Ek 6’da verilmiştir.

Nmap aracının içerisinde bulunan bu kod parçacığı sayesinde memcached sunucuları için “status” komutu çalıştırılmaktadır. Bilgilerin gizlenmiş olduğu bir IP için yapılan nmap taramasının örnek çıktısı şekil 3.1 de gösterilmiştir.

Şekil 3.1: Memcached “status” bilgilerinin alınması



3. TARAMA SONUÇLARI

Yapılan taramalar ve detaylı incelemeler neticesinde saldırılarda yükseltici olarak kullanılabilecek çok sayıda sunucu keşfedilmiştir. Sonuçlar ülkeler genelinde sıkılaştırma bilincini göstermesinin yanı sıra saldırganlar için hali hazırda yeteli miktarda erişilebilir saldırı aracıları bulunduğunu göstermektedir. Protokoller özelinde sonuçların ele alınma durumları aşağıda gösterilmiştir.

3.1 Dns Yükseltici Sonuçları

Yapılan çalışmalar esnasında 4,710,156 adet port 53 üzerinden yayın yapan sunucu ile karşılaşılmıştır. Yükseltici olup olmamalarını araştırmak için yapılan sorguların önemli bir bölümünde bağlantı sağlanamama durumu ile karşılaşılmıştır. Bu sayı 2,922,529 iken 1,279,939 adet sunucunun beklenilen sıkılaştırmayı yapması ile birlikte 4,202,468 DNS sunucusunun yükseltici olarak kullanılamaz durumda olduğu tespit edilmiştir. Doğru sıkılaştırmalar sonucu sorgu yapan tarafa gönderilen cevap Şekil 4.1'de gösterilmiştir.

```
root@ubuntu:/home/mercan# nslookup -timeout=4 -retry=1 -q=ANY www.etu.edu.tr 109.68.105.194
Server:         109.68.105.194
Address:        109.68.105.194#53

** server can't find www.etu.edu.tr: REFUSED
```

Şekil 4.1: Sıkılaştırılmış DNS sunucu cevap örneği

Sıkılaştırmaların yapılmadığı ya da eksik olarak yapıldığı DNS sunucuları ele alınacak olursa bunlardan en az zarar verebilecek olan sorgulanan alan adının sadece IPv6 bilgisini veren sunucular olduğu görülmektedir. Bu şekilde eksik sıkılaştırma yapılmış olan sunucu sayısı 226,002'dir.

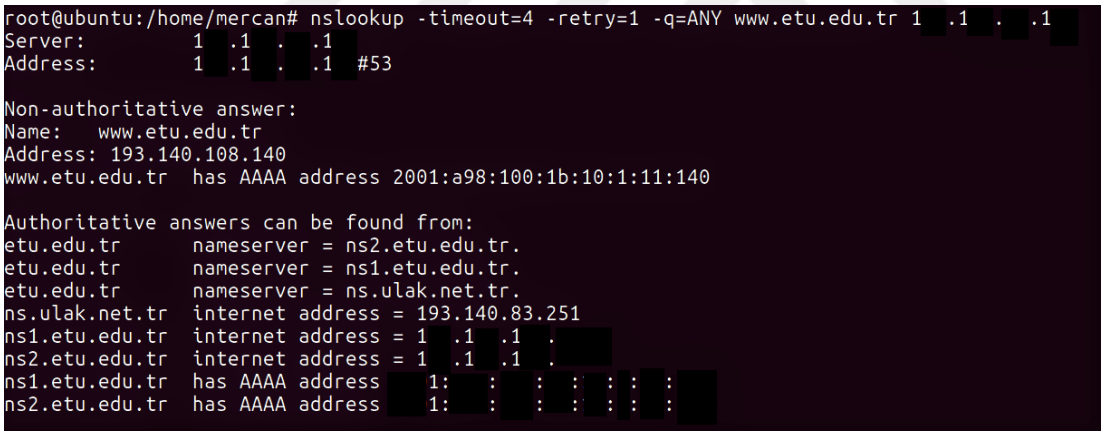
Yetkili olmayan açık çözümleyicilerde gözlemlenen bu durum diğer DNS yükselticilerine istinaden çok düşüktür. Şekil 4.2'de verilen www.etu.edu.tr alanı için

bu şekilde tedbirler alınmış sunucuya gerçekleştirilen sorgu, yansıtıcının IP adresi gizlenerek gösterilmiştir.

Şekil 4.2: Sorgulara istinaden alan adı ile sadece sorgu yapılan etki alanının IPv6 adresinin verildiği yükselticiler.

Yapılan sorgulara cevap olarak, sorgu yapılan alan ile ilgili tüm verilerin dönülmesi ise saldırılar için daha büyük bir güç sağlamaktadır. Yapılan çalışmada, bu şekilde açıklık barındıran sunucu sayısının 34,571 olduğu gözlenmiştir.

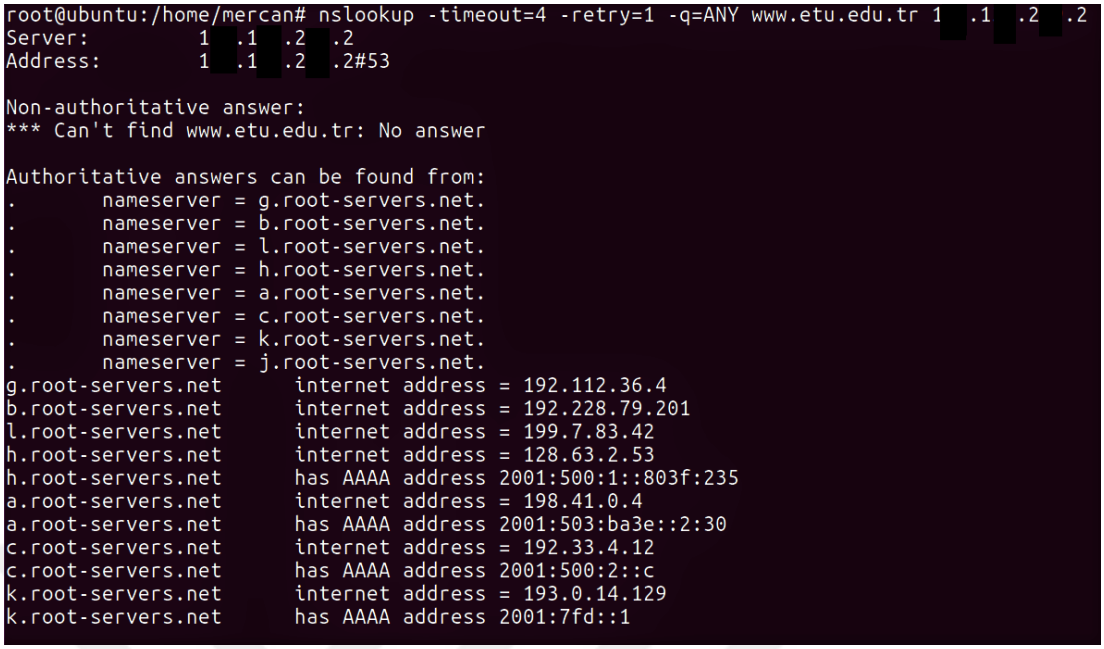
Şekil 4.3'de www.etu.edu.tr alanı için yapılan bir sorgu, yansıtıcının IP adresi ve üniversitenin kayıtlı bilgileri gizlenerek gösterilmiştir.



Şekil 4.3: Sorgulara istinaden alan adı ile ilgili tüme verilerin cevap olarak verildiği yükselticiler

Yapılabilecek saldırılar açısından en büyük risklerden bir tanesini ise ilgili sorguya yanıtın nereden bulunabileceği detaylarının verildiği sunuculardan gelen yanıtlardır. Bazı durumlarda eldeki bilgileri vermekten daha yüksek yükseltici faktörüne sahip olabilecek bu sunuculardan 72,564 adet tespit edilmiştir.

Şekil 4.4'te www.etu.edu.tr alanı için bu şekilde tedbirler alınmış sunucuya gerçekleştirilen sorgu, yansıtıcının IP adresi ve diğer önem arz edebilecek bilgiler gizlenerek gösterilmiştir.



Şekil 4.4: Sorgulara istinaden kök sunucu adreslerinin cevap olarak verildiği yükselticiler.

Yapılan çalışmanın kapsadığı ülkeler dâhilinde 347,164 adet DRDoS saldırılarında yükseltici olarak kullanılabilecek DNS sunucusu tespit edilmiştir. Elde edilen sunucular ülkeler arasında dengeli bir şekilde dağılım göstermemektedir. DNS sunucu sayılarını ülkeler özelinde değerlendirdiğimiz zaman en fazla DNS sunucusu İspanya'da keşfedilirken en az DNS sunucusu kapsam dâhilde olan ülkeler arasında Lihtenştayn'da keşfedilmiştir. Yükseltici olarak kullanılabilecek sunucuların ülkeler genelinde dağılımı Çizelge 4.1'de verilmiştir. Bu çizelgede yapılan "ANY" sorgusuna cevaben alan adına ait IPv6 bilgilerini veren sunucular, alan adı ile ilgili tüm bilgileri veren sunucular ve kök bilgileri veren sunucular ayrı ayrı ele alınmış en fazla DNS yükselticisi keşfedilen ülkeden en az sayıda yükseltici keşfedilmiş ülkeye doğru sıralanmıştır. Bazı ülkeler için keşfedilen DNS sunucusunun yükseltici olarak kullanılabilme ihtimali çok yüksek iken bazı ülkelerde durumun tam tersi olduğu görülmüştür.

Çizelge 4.1: DNS Yükselticilerini verdiği yanıtlara göre dağılımları.

Ülke Adı	DNS Sunucusu Sayısı	Sadece IPv6 Bilgisi	Kök Bilgisi	Kayıtlı Bilgi
Almanya	406282	13188	6096	6096
Andorra	486	30	24	24
Arnavutluk	3410	326	291	291
Avusturya	19651	1367	585	585
Belarus	4944	591	297	297
Belçika	82171	838	354	354
Birleşik Krallık	325067	34384	6563	6563
Bosna Hersek	6948	248	171	171
Bulgaristan	130017	14837	1953	1953
Çekya	70802	3558	1421	1421
Danimarka	14336	822	344	344
Ermenistan	8467	284	225	225
Estonya	10437	410	147	147
Finlandiya	53993	1242	203	203
Fransa	438344	12682	3673	3673
Hırvatistan	75877	280	362	362
Hollanda	209751	5342	3422	3422
İrlanda	13426	926	360	360
İspanya	990684	4636	2116	2116
İsveç	109745	9144	1458	1458
İsviçre	31275	2422	769	769
İtalya	238688	23412	2737	2737
İzlanda	2376	131	67	67
Karadağ	817	466	34	34
K. Makedonya	2587	159	113	113
Letonya	18698	685	648	648
Lihtenştayn	393	27	16	16
Litvanya	20143	620	413	413
Lüksemburg	2917	128	56	56
Macaristan	28301	1564	980	980
Malta	9413	147	74	74
Moldova	11697	1740	210	210
Norveç	46200	1724	381	381
Polonya	140181	9125	3909	3909
Portekiz	27289	2012	559	559
Romanya	153822	8635	2003	2003
Rusya	573916	32909	11786	11786
Sırbistan	21683	1266	924	924
Slovakya	15138	1042	660	660
Slovenya	7009	333	355	355
Türkiye	234003	28244	10571	10571
Ukrayna	133452	16143	4879	4879
Yunanistan	15320	1121	355	355

Çizelge 4.2’de ülkeler çapında keşfedilen DNS sunucularının sayısı ve yükseltici olarak kullanılabilecek sunucu sayıları gösterilmiştir. Çizelge oransal olarak yükseltici ile karşılaşılabileceği ihtimalinin en düşük olduğu ülkeden en yüksek olduğu ülkeye doğru sıralanmıştır.

İstatistiksel olarak keşfedilen bir DNS sunucusunun yükseltici olarak kullanılabilmesinin ihtimalinin en düşük olduğu ülke İspanya olarak tespit edilmiştir. İspanya’ nın yanı sıra Hırvatistan’ da keşfedilen DNS sunucularının da büyük bir kısmı yükseltici olarak kullanılamaz durumdadır. İspanya da keşfedilen her 1000 DNS sunucusundan 7 tanesi yansıtıcı olarak kullanılabilir durumdayken bu sayı Karadağ’ da bu sayı 645’ dir.

Çizelge 4.2: DNS sunucusu başına düşen yükseltici sayısı ve oranı

Ülke Adı	Sunucusu Sayısı	Yükseltici Sayısı	Sunucu Başına Düşen Yükseltici
İspanya	990684	7167	0.007234396
Hırvatistan	75877	711	0.009370428
Belçika	82171	1331	0.016197929
Malta	9413	227	0.024115585
Finlandiya	53993	1546	0.028633341
Hollanda	209751	9168	0.043708969
Fransa	438344	19322	0.044079536
Norveç	46200	2365	0.051190476
Almanya	406282	21123	0.051990982
Estonya	10437	653	0.062565871
Litvanya	20143	1357	0.067368317
Lüksemburg	2917	212	0.072677408
Romanya	153822	11452	0.074449689
Bosna Hersek	6948	581	0.083621186
Çekya	70802	6207	0.087667015
Ermenistan	8467	755	0.089169718
Rusya	573916	53131	0.092576266
İzlanda	2376	230	0.096801347
Letonya	18698	1818	0.09722965
İrlanda	13426	1353	0.100774616
Portekiz	27289	2846	0.104291106
Polonya	140181	15083	0.107596607
İsveç	109745	11859	0.108059593
Slovenya	7009	773	0.110286774
Andorra	486	54	0.111111111
İsviçre	31275	3613	0.115523581
İtalya	238688	27935	0.117035628
Avusturya	19651	2334	0.118772582
Danimarka	14336	1726	0.120396205
Macaristan	28301	3469	0.122575174
Yunanistan	15320	1916	0.125065274
Birleşik Krallık	325067	42786	0.131622096
Bulgaristan	130017	17644	0.135705331
Lihtenştayn	393	58	0.147582697
K. Makedonya	2587	405	0.156551991
Slovakya	15138	2425	0.160192892
Türkiye	234003	40310	0.172262749
Ukrayna	133452	23003	0.172369092
Moldova	11697	2207	0.188680858
Belarus	4944	1039	0.210153722
Sırbistan	21683	4660	0.21491491
Arnavutluk	3410	785	0.230205279
Karadağ	817	525	0.642594859

Konu ile ilgili ele alınabilecek bir diğer husus ise sıkılaştırılmış sunucu başına düşen yükseltici sayısıdır. Tüm erişim problemleri göz ardı edildiğinde saf sıkılaştırma bilincini verecek oranlar ele alındığında; Hollanda ve Fransa' nın yüksek başarı oranları dikkat çekmektedir. Bu ülkelerle beraber Estonya'nın 2007'de yaşadığı saldırıdan sonra yaptığı sıkı çalışmaların neticesi burada kendini göstermektedir.

Hollanda ve Fransa' da bağlantı problemi yaşanmamış her 12 DNS sunucusundan 11 tanesi sıkılaştırılmış durumdadır. Bu ülkelerin yanı sıra Estonya ve Almanya' da bağlantı sağlanan her 11 sunucunun 10' u sıkılaştırılmış durumdadır. İstatistiksel olarak keşfedilmiş sunucunun yükseltici çıkma olasılığının en düşük olduğu ülke İspanya her 10 cihazın 9' unun sıkılaştırılmış olması ile yine ilk sıralarda yer almıştır. Türkiye' de bağlantı sağlanan her 3 DNS sunucusunun 2' si sıkılaştırılmış durumdayken istatistiksel olarak en başarısız olarak tespit edilmiş Karadağ' da her 11 sunucunun sadece 1 tanesinin sıkılaştırılmış olduğu tespit edilmiştir.

Çizelge 4.3'de sıkılaştırılmış sunucu başına düşen yükseltici sayısı ele alınmıştır. Çizelgede sıkılaştırma sonuçlarının en başarılı olarak gözlemlendiği ülkelerden başarısız ülkelere doğru sıralama yapılmıştır.

Çizelge 4.3: Sıkılaştırılma yapılmış DNS sunucusu başına düşen yükseltici sayısı.

Ülke Adı	Sıkılaştırılmış Sunucu Sayısı	Yükseltici Sayısı	Sıkılaştırılmış Sunucu / Yükseltici
Hollanda	107136	9168	11.68586387
Fransa	221296	19322	11.45305869
Estonya	6941	653	10.62940276
Almanya	199513	20123	9.91467475
Litvanya	11960	1357	8.813559322
İspanya	63164	7167	8.81317148
Malta	1387	227	6.110132159
Lüksemburg	1204	212	5.679245283
İzlanda	1099	230	4.77826087
İsveç	54561	11859	4.600809512
Romanya	52281	11452	4.565228781
Norveç	10666	2365	4.509936575
Bulgaristan	71448	17644	4.0494219
Slovenya	3031	773	3.921086675
Portekiz	10567	2846	3.712930429
İsviçre	13148	3613	3.639081096
İrlanda	4879	1353	3.606060606
Belçika	4195	1331	3.15176559
Çekya	18192	6207	2.930884485
Finlandiya	4126	1546	2.668822768
Letonya	4591	1818	2.52530253
Hırvatistan	1716	711	2.41350211
Avusturya	5533	2334	2.370608398
Macaristan	8105	3469	2.336408187
Bosna Hersek	1352	581	2.327022375
Rusya	117651	53131	2.214356967
Polonya	32587	15083	2.160511835
Yunanistan	3849	1916	2.008872651
Birleşik Krallık	85637	42786	2.001519189
Danimarka	3287	1726	1.904403244
Türkiye	73317	40310	1.818829075
Lihtenştayn	101	58	1.74137931
Slovakya	3598	2425	1.48371134
İtalya	41235	27935	1.476105244
Belarus	1522	1039	1.464870067
Moldova	3142	2207	1.423652016
Ukrayna	27882	23003	1.212102769
Andorra	51	54	0.944444444
Kuzey Makedonya	311	405	0.767901235
Ermenistan	522	755	0.691390728
Sırbistan	2721	4660	0.583905579
Arnavutluk	372	785	0.47388535
Karadağ	63	525	0.12

3.2 NTP Yükseltici Sonuçları

Yapılan çalışmalar esnasında 3,421,556 adet port 123 üzerinden yayın yapan sunucu ile karşılaşıldı. Bu sunucuların büyük bir çoğunluğunun sıkılaştırıldığını gözlemlendi. İlk sıkılaştırma gereksinimlerinin 2013 senesinde belirtilmiş olmasına karşın hala 5,134 adet NTP sunucusunun sıkılaştırılmamış ya da eksik sıkılaştırılmış durumda olduğu tespit edildi ve tespit edilen sunucu sayılarının ülkelere göre büyük değişiklikler göstermekte olduğu görüldü.

Çalışma kapsamında elde edilen sunucuların yaklaşık olarak %21'inin (724,083) İtalya'da bulunduğu görüldü. Almanya, Rusya ve İtalya'da keşfedilen sunucu sayıları tüm ülkeler kapsamında elde edilen sunucu sayısının yaklaşık olarak %49'una denk geldiği izlendi.

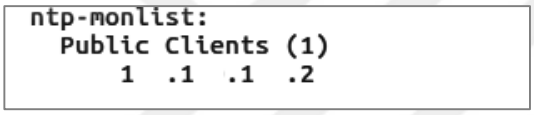
NTP sunucuların ülkeler genelinde dağılımı Çizelge 4.4'de verilmiştir. Çizelgede ülkeler en çok NTP sunucusu barındıran ülkeden en az NTP sunucusu barındıran ülkeye doğru sıralanmıştır. NTP sunucularının DRDoS saldırılarında yükseltici olarak kullanılabilme durumu incelendiğinde, iki yükseltici durumu karşımıza çıkmaktadır. İlk durum herhangi bir sıkılaştırmanın yapılmamış olması durumudur. İkinci durum ise yetersiz tedbirlerin alınması sonucu sadece belirli bilgilerin geri dönüş yaptığı durumdur.

Çizelge 4.4: Ülkeler bazında NTP sunucusu dağılımı.

Ülke Adı	NTP Sunucu Sayısı
İtalya	724083
Rusya	525551
Almanya	409388
Birleşik Krallık	286877
Fransa	266694
Hollanda	135962
İsviçre	112763
Romanya	95904
İsveç	90982
Türkiye	77436
İspanya	70602
Polonya	70118
Çekya	65614
Ukrayna	60783
Portekiz	45223
Norveç	42988
Danimarka	38090
Belçika	37806
Bulgaristan	36811
Avusturya	34875
Slovakya	26604
Yunanistan	24983
Finlandiya	21640
Sırbistan	16017
Belarus	15907
İrlanda	10313
Moldova	10041
Hırvatistan	8836
Kuzey Makedonya	8519
Slovenya	8387
Estonya	6792
Macaristan	6096
İzlanda	5905
Arnavutluk	5775
Litvanya	3584
Bosna Hersek	3308
Lüksemburg	3267
Malta	2863
Ermenistan	2306
Karadağ	1048
Letonya	349
Lihtenştayn	331
Andorra	141

Yetersiz sıkılaştırmaların yapıldığı NTP sunucuları “monlist” sorgusuna açık olmasına karşın sadece kendisine bağlı olan IP adreslerini sonuç olarak getirmektedir. Bu durum hiç sıkılaştırılmamış sunucuların etkilerinin daha az olma potansiyelini güçlendirmektedir. Buna karşın yapılan çalışmaların sonucunda, bazı yetersiz sıkılaştırma yapılmış sunucuların, kendilerine çok fazla cihazın bağlı olmasından dolayı, hiç sıkılaştırma yapılmamış sunuculardan daha fazla yükseltici faktörüne sahip olduğu görülmüştür.

Şekil 4.5’de kendisine bağlı cihaz sayısı çok az olan ve üzerinde belirli sıkılaştırmaların yapılması sonucunda sadece IP adreslerinin alınabildiği sunucu örneği verilmiştir. Saldırganlar için bu örnekteki sunucu, yükseltici olarak kullanılabilmektedir, ancak çok düşük yükseltici faktörüne sahiptir.



Şekil 4.5: Az sayıda etkileşimde olan yetersiz sıkılaştırma yapılmış NTP sunucusunun monlist sorgu yanıtı.

Şekil 4.6’da ise yetersiz sıkılaştırmaların yapıldığı ancak kendisine çok fazla cihaz bağlı olan sunucunun verdiği cevap gösterilmektedir. Bu sunucu ile irtibatta olan 578 cihazın sadece bir kısmı gösterilmiştir.

Şekil 4.7’de ise kendisine bağlı cihaz sayısı az olan ancak sıkılaştırma yapılmamış olan NTP sunucusu gösterilmektedir. Şekil 4.6 ile 4.7 kıyaslandığında şekil 4.6’da geçen sunucuda belirli sıkılaştırmaların yapılmış olmasına karşın, şekil 4.7’de ele alınan sunucunun daha büyük bir yükseltici faktörüne sahip olduğu görülmektedir.

```
ntp-monlist:
  Target is synchronised with 1   .1   .1.0
  Alternative Target Interfaces:
      1   .1   .1.2
  Public Clients (588)
      1.6 .2  209       9.1  .5 .2      1  . 0.1  .1     1  .3 .6 .2
      1.1  .1  .2       9.1  .3 .9      1  . 8 .1  .2    1  .3 .6 .2
      2.5 .4 .1         0.8 .7 .3       1  . 4 .1  .1    1  .7 .1  .2
      2.2  .2  .1       0.8 .7 .1       1  . 4 .2 .1     1  .9 .1  .1
      3.8 .8.1          1.2 .1  .1      1  . 4 .3 .1     1  .9 .1  .1
      3.8 .1 .1         1.1  .2  .4     1  . 5 .1  .1    1  .1  .   .3
      3.8 .2 8.6        1.2  .2  .1     1  . 1 .1  .2    1  .1  .   .3
      3.8 .2 6.6        1.2  .1 6.1     1  . 3.16 .1     1  .1  .  .1
      3.9 .5 .7         2.2 .2  .1      1  . 7.12 .1     1  .1  .  9.1
      3.9 .2  .9        2.1  .2  .8     1  . 2 .1  .9    1  .1  .  1.1
      4.1  .1  .2       2.1  .1.7       1  . 9.4 .4      1  .2  . .4
      4.2  .2  .2       2.2  .1  .6     1  . 4 .1  .1    1  .2  . 5.1
      5.6 .9 .2         3.4 .1  .0      1  . 4 .3 .2     1  .2  . 5.1
      5.7 .4 .2         3.1  .2  .3     1  . 4 .1  .2    1  .2  . 6.2
      6.6 .1 7.1        3.1  .2  .2     1  . 6 .1  .8    1  .2  . 5.1
      1 .1 .2  .6       3.1  .1 .1      1  . 4 .1  .7    1  .2    .2
      1 .1 .2  .1       4.6   .1        1  . .3 .8       1  .1  . 4 .2
      1 .2 .1 .2        4.8   .1        1  . 5 .2  .1    1  .1  . 8.1
      1 .2  .3 .1       4.3 .2 1.2      1  . 6 .2  .1    1  .1  . 2 .3
      1 .2  .1 .1       4.7 .6 .2       1  . 1.1  .22    1  .1  . 6.1
      1 .1 .8.4         4.1  .2  .2     1  . 4 .2  .1    1  .1  . 9 .1
      1 .2 .4 .2        4.2  .1.2       1  . 1 .1  .1    1  .2  . 9.1
      1 .7 .2  .3       5.1  .1  .1     1  . 7.1  .17    1  .1  . 4.1
      1 .1  .8 .2       5.1  .2  .2     1  . 2 .4 .21    1  .1  . 9.2
      1 .1 .9 .2        6.5 .14 .13     1  . .5 .1       1  .2 .2 7.2
      1 .7 .1  .1       6.1  .2 4.1     1  . 8.2  .2     1  .9 .2 4.5
      1 .1  .1  .       7.2  .3 .8      1  . 8.2  .4     1  .9 .2 4.41
      1 .2  .1  .       8.1  .1.73      1  . 8.2  .12    1  .1  . 2 .1
      1 .2  .1  .       8.1  .6 .1      1  . 8.2  .13    1  .2  . 0 .2
      1 .8 .1  .9       8.2  .6 .1      1  . 8.2  .16    1  .7 .9 1
      1 .9 .1  .2       9.8 .1  .7      1  . 8.2  .17    1  .2 0.1  .2
      1 .2  .2.7        9.1  .1  .1     1  .8 .2  .1     1  .2  .7 .8
      2 .1  .4 .4       9.1  .3 .1      1  .8 .2  .1     1  .2  .1  .2
      2 .1 .1  .2       9.2  .1  .1     1  .8 .2  .2     1  .1  .1  .2
      2 .7 .3 .6        1.  .2  .8      1  .8 .2  .2     1  .2  .1  .1
      2 .1  .1  .1      1.  .5 .1       1  .8 .2  .2     1  .1  .3 .2
      2 .1  .2  .1      1.   .1  .4     1  .8 .2  .2     1  .1  .3 .1
      2 .2  .1  .5      1.   .1  .1     1  .8 .2  .2     1  .2  .1  .2
      3 .2  .1  .4      2. .2  .1       1  .8 .2  .2     1  .1     .5
      3 .4 .1  .1       2.4 .1  .2      1  .8 .2  .2     1  .5    .5
      3 .9 .1  .2       2.1  .  2.9     1  .8 .2  .2     1  .5    .5
      3 .1  .2  .1      3.4 .1  .2      1  .8 .2  .2     1  .5    .5
      3 .1.1 .7         5.2.1 .8        1  .8 .2  .3     1  .5    .5
      3 .2 .7 .1        6.   .1  .2     1  .8 .2  .3     1  .5    .6
      3 .3 .1  .1       6.   .1 .2      1  .8 .2  .3     1  .5    .6
      3 .4 .1  .1       6.   .9 .1      1  .8 .2  .3     1  .5    .6
      3 .1  .6 .2       7.4 .1  .2      1  .8 .2  .3     1  .5    .6
      3 .1  .1  .3      8. .2  .2       1  .8 .2  .3     1  .5    .6
      3 .1  .2  .1      8.1  .8 .7      1  .8 .2  .3     1  .5    .8
      3 .2  .1  .1      8.1  .6 .1      1  .8 .2  .4     1  .5    .8
      3 .7 .2  .1       8.2  .1  .1     1  .8 .2  .4     1  .5 .4 .9
```

Şekil 4.6: Çok sayıda etkileşimde olan yetersiz sıkılaştırma yapılmış NTP sunucusunun monlist sorgu yanıtı.

Şekil 4.8 de ise hem sıkılaştıma yapılmamış hem de kendisine çok fazla cihazın bağlı olduğu bir NTP sunucusu örnek gösterilmiştir.

```
ntp-monlist:
  Target is synchronised with 1 .2  .3 .1
  Alternative Target Interfaces:
      1  .1  .2.9
  Public Servers (1)
      1 .2  .3 .1
  Other Associations (1)
      1  .1   1  .2 (You?) seen 4 times. last tx was unicast v2 mode 7
```

Şekil 4.7: Az sayıda etkileşimde olan sıkılaştırılmamış NTP sunucusunun monlist sorgu yanıtı.

43 ülke genelinde yapılmış olan yansıtıcı dağılımları Çizelge 4.5'te gösterilmiştir. Çizelge içerisinde geçen sadece IP bilgisi sütunu Şekil 4.4 ve Şekil 4.5 örneklerinde de gösterilmiş olan, kendisine bağlanmış IP adreslerini veren NTP sunucularıdır. Tüm monlist bilgisi sütununda ise Şekil 4.6 ve Şekil 4.7'de örnekleri bulunan cevap formatına dönüş yapan sunucu sayıları gösterilmiştir.

Üç binden fazla NTP sunucusu barındıran Lüksemburg'da, binden fazla NTP sunucusu barındıran Karadağ'da ve 331 adet NTP sunucusu barındıran Lihtenştayn'da NTP saldırılarında yansıtıcı olarak kullanılabilecek bir yansıtıcı keşfedilememiştir. Bu ülkeler haricinde 6,792 adet NTP sunucusu keşfedilen Estonya'da sadece 1 adet yükseltici tespit edilmiştir. İstatistiksel olarak NTP sunucularının sıkılaştırılması konusunda en başarısız ülkeler: Letonya, Türkiye ve Andorra olarak sıralanmaktadır. NTP sunucusu başına düşen yükseltici oranında en başarısız 4. ülke olan İspanya ile Türkiye kıyaslandığı zaman İspanya'nın iki kat daha başarılı olduğu görülmektedir.

```
ntp-monlist:
  Alternative Target Interfaces:
      1  .1  .1.2
  Public Clients (1)
      1  .8 .2  .4
  Other Associations (587)
       3.1  .1  .2 (You?) seen 3 times. last tx was unicast v2 mode 7
       0.9 .2 .1   seen 21651 times. last tx was unicast v2 mode 7
      6.9 .6 .5  seen 2455 times. last tx was unicast v2 mode 7
       5.2  .1 .1   seen 133099 times. last tx was unicast v2 mode 7
      5.3 .8 .4 seen 4054 times. last tx was unicast v2 mode 7
       0.2.1  .2  seen 6428 times. last tx was unicast v2 mode 7
      1 .1  .8 .2   seen 1 time. last tx was unicast v2 mode 7
      2.2   4 .8  seen 1911 times. last tx was unicast v2 mode 7
      1.1 .1  .1   seen 11648 times. last tx was unicast v2 mode 7
      5.6 .1 .6  seen 9 times. last tx was unicast v2 mode 7
      6.2 1.2  .1   seen 263 times. last tx was unicast v2 mode 7
     5.3 .1 .1   seen 2746 times. last tx was unicast v2 mode 7
       7.7 .9 .1   seen 621 times. last tx was unicast v2 mode 7
       3.3 .1 .1   seen 1 time. last tx was unicast v0 mode 7
       6.2  .43.4  seen 215 times. last tx was unicast v2 mode 7
      6.4.1 .7  seen 1219 times. last tx was unicast v2 mode 7
      7 .2  .1 .1   seen 721 times. last tx was unicast v2 mode 7
      9.163.1  .1   seen 175 times. last tx was unicast v2 mode 7
      6.2 .4 .1   seen 7733 times. last tx was unicast v2 mode 7
       5.1  .3 .7 seen 6262 times. last tx was unicast v2 mode 7
       9.2  .1  .1   seen 13575 times. last tx was unicast v2 mode 7
       3.2  .2  .1   seen 98060 times. last tx was unicast v2 mode 7
       7.5 .1  .1   seen 3818 times. last tx was unicast v2 mode 7
      2.2  .2 .1   seen 2153 times. last tx was unicast v2 mode 7
       7.1  .1  .8  seen 112 times. last tx was unicast v2 mode 7
       3.1  .9 .5  seen 42146 times. last tx was unicast v2 mode 7
      5.2  .1  .4  seen 1309 times. last tx was unicast v2 mode 7
      7.2  .2  .1   seen 7178 times. last tx was unicast v2 mode 7
       5.2  .1  .1   seen 6546 times. last tx was unicast v2 mode 7
      3.6 .1 .2   seen 13955 times. last tx was unicast v2 mode 7
      2 .7 .1  .2   seen 58980 times. last tx was unicast v2 mode 7
      8 .2  .2  .6  seen 954 times. last tx was unicast v2 mode 7
      5.2  .9 .5  seen 4954 times. last tx was unicast v2 mode 7
       7.1  .5 .7  seen 6297 times. last tx was unicast v2 mode 7
       1. 7.4.2   seen 2619 times. last tx was unicast v2 mode 7
     ?.2  .1 .8 seen 7642 times. last tx was unicast v2 mode 7
      7.6.156.7  seen 629 times. last tx was unicast v2 mode 7
      0 .8 .1  .2   seen 5656 times. last tx was unicast v2 mode 7
      4 .7 .1  .1  seen 1 time. last tx was unicast v2 mode 7
      0.2 .1  .6  seen 2205 times. last tx was unicast v2 mode 7
      1 .6 .2 .9 seen 39557 times. last tx was unicast v2 mode 7
       2.1  .3 .1   seen 1 time. last tx was unicast v2 mode 7
       0.5 .2  .1   seen 3827 times. last tx was unicast v2 mode 7
       0.1  .2  .1   seen 20501 times. last tx was unicast v2 mode 7
       2.1  .2  .4  seen 1825 times. last tx was unicast v2 mode 7
       5.7.0.4  seen 3 times. last tx was unicast v2 mode 7
      4.6 .5 .1  seen 12095 times. last tx was unicast v2 mode 7
       7.1  .1  .2  seen 5680 times. last tx was unicast v2 mode 7
      2.1  .4.1   seen 8298 times. last tx was unicast v2 mode 7
       7.5 .1  .1   seen 8037 times. last tx was unicast v2 mode 7
```

Şekil 4.8: Çok sayıda etkileşimde olan sıkılaştırılmamış NTP sunucusunun monlist sorgu yanıtı.

Çizelge 4.5: NTP yükselticilerinin ülkeler özelinde dağılımı.

Ülke Adı	Sadece IP Bilgisi	Tüm MONLIST Bilgisi
Almanya	85	21
Andorra	1	1
Arnavutluk	2	2
Avusturya	64	5
Belarus	4	2
Belçika	24	6
Birleşik Krallık	148	31
Bosna Hersek	3	0
Bulgaristan	28	4
Çekya	43	14
Danimarka	8	1
Ermenistan	5	2
Estonya	1	0
Finlandiya	34	4
Fransa	558	46
Hırvatistan	4	0
Hollanda	90	23
İrlanda	5	2
İspanya	739	115
İsveç	50	12
İsviçre	17	1
İtalya	262	45
İzlanda	3	1
Karadağ	0	0
Kuzey Makedonya	5	0
Letonya	12	5
Lihtenştayn	0	0
Litvanya	11	2
Lüksemburg	0	0
Macaristan	29	2
Malta	2	0
Moldova	5	1
Norveç	114	12
Polonya	95	22
Portekiz	64	14
Romanya	19	7
Rusya	153	27
Sırbistan	7	0
Slovakya	8	2
Slovenya	4	0
Türkiye	1865	16
Ukrayna	27	12
Yunanistan	67	9

Hatalı ya da eksik sıkılaştırma olarak ele alınan, sunucuya bağlanmış cihazların sadece IP adreslerinin dönüşü, Türkiye sunucularında çok fazladır. Sadece IP bilgisinin dönüyor olmasının yükseltici olmaya yetmesine karşın, ilgili tüm kayıtların cevap olarak gönderilmesi kritik bir husustur. Bu konuda İspanya' da 115 adet detaylı bilgileri dönüş yapan sunucu keşfedilmiştir.

Çizelge 4.6'da NTP sunucusu başına düşen yükseltici oranı gösterilmektedir ve NTP sunucusu başına düşen yükseltici oranının en az olduğu ülkeden en çok olduğu ülkeye doğru sıralanmıştır.

Çizelge 4.6: Ülkeler özelinde NTP sunucusu başına düşen yükseltici sayısı.

Ülke Adı	NTP Sunucusu Sayısı	Yükseltici Sayısı	Sunucu Başına Düşen Yükseltici Sayısı
Karadağ	1048	0	0
Lihtenştayn	331	0	0
Lüksemburg	3267	0	0
Estonya	6792	1	0.000147232
İsviçre	112763	18	0.000159627
Danimarka	38090	9	0.000236282
Almanya	409388	106	0.000258923
Romanya	95904	26	0.000271104
Rusya	525551	180	0.000342498
Slovakya	26604	10	0.000375883
Belarus	15907	6	0.000377192
Sırbistan	16017	7	0.000437036
Hırvatistan	8836	4	0.000452694
Slovenya	8387	4	0.000476929
İtalya	605936	307	0.000506654
K. Makedonya	8519	5	0.000586923
Moldova	10041	6	0.00059755
Birleşik Krallık	286877	179	0.000623961
Ukrayna	60783	39	0.000641627
İzlanda	5905	4	0.000677392
İrlanda	10313	7	0.000678755
İsveç	90982	62	0.000681453
Arnavutluk	5775	4	0.000692641
Malta	2863	2	0.000698568
Belçika	37806	30	0.000793525
Hollanda	135962	113	0.000831115
Çekya	65614	57	0.000868717
Bulgaristan	36811	32	0.000869305
Bosna Hersek	3308	3	0.000906892
Polonya	70118	117	0.001668616
Portekiz	45223	78	0.001724786
Finlandiya	21640	38	0.001756007
Avusturya	34875	69	0.001978495
Fransa	266694	604	0.002264768
Norveç	42988	126	0.002931051
Ermenistan	2306	7	0.003035559
Yunanistan	24983	76	0.003042069
Litvanya	3584	13	0.003627232
Macaristan	6096	31	0.005085302
İspanya	70602	854	0.012095975
Andorra	141	2	0.014184397
Türkiye	77436	1881	0.024291027
Letonya	349	17	0.048710602

Ülke çapında bulunan toplam NTP sunucularının ele alınarak yapıldığı çalışma Estonya, İsviçre ve Danimarka' yı ön plana çıkarmaktadır. NTP sunucuları çalışma kapsamında en çok sıkılaştırılmış servis olarak dikkat çekmektedir. Çalışma kapsamında 30 ülkede yansıtıcı oranı 1/1000 in altındadır. Bu oranlar İspanya' da 12/1000, Türkiye' de 24/1000 ve Letonya' da 48/1000 olarak tespit edilmiştir. En kötü sıkılaştırma oranına sahip Letonya ile sadece bir tane yükseltici keşfedilen Estonya karşılaştırıldığında ise Estonya'nın başarı oranının 331 kat daha iyi olduğu görülmektedir.

3.3 Memcached Yükseltici Sonuçları

Yapılan çalışmalar neticesinde 43 ülkede 615,023 adet TCP port 11211 üzerinden yayın yapan sunucu keşfedilmiştir. 146.667 adet memcached sunucusu bulunan Birleşik Krallık'ın çalışma kapsamında bulunan 43 ülke arasında en yüksek rakama sahip olduğu görülmüştür. Çizelge 4.7'de ülkeler özelinde memcached sunucularının dağılımı ele alınmıştır. Yapılan araştırmalar sonucunda 4,238 adet yükseltici keşfedilmiştir. Yükseltici sayıları çizelge 4.8'de gösterilmiştir. Bu çizelge en az yükseltici keşfedilen ülkeden en çok keşfedilen ülkeye doğru sıralanmıştır. Çalışmaların ışığında en fazla yükselticinin Rusya'da olduğu görülmüştür. Bununla beraber ülkeler özelinde keşfedilen memcached sunucusu başına düşen yükseltici sayısı Çizelge 4.9'da ele alınmıştır. Burada en dikkat çekici husus ise Litvanya'da tespit edilen sunucuların %79'dan daha fazla bir oranda hali hazırda UDP protokolünü desteklemesidir. İnternete açık olmaları gereksinimlerinin tespit etmek servis yöneticileri ile görüşmeden imkansız olarak değerlendirilmektedir. Bu sebepten ötürü memcached özelinde bu sonuçların başarı konusunda net bir gösterge olmamasıyla birlikte, sunucu yöneticilerinin kullandıkları sistemi güncel halde tutma kabiliyetlerini net bir şekilde ortaya koymaktadır.

Çizelge 4.7: Memcached sunucularının ülkeler özelinde dağılımı.

Ülke Adı	Memcached Sunucu Sayısı
Birleşik Krallık	146677
Fransa	129797
Hırvatistan	64871
Almanya	42658
Finlandiya	32500
İtalya	27901
Romanya	26864
Polonya	25031
Hollanda	19430
Belçika	13962
Türkiye	11719
Rusya	9863
Norveç	9216
İspanya	8907
Danimarka	8703
Letonya	8212
İsveç	6557
Çekya	5290
Estonya	4313
Avusturya	3932
İsviçre	2060
Ukrayna	1284
Slovenya	960
Macaristan	770
Yunanistan	698
İzlanda	693
Bulgaristan	513
Litvanya	430
Slovakya	242
Portekiz	226
İrlanda	185
Sırbistan	115
Lüksemburg	110
Moldova	70
Ermenistan	47
Kuzey Makedonya	46
Belarus	43
Malta	40
Bosna	39
Arnavutluk	35
Karadağ	11
Lihtenştayn	2
Andorra	1

Çizelge 4.8: Memcached yükselticilerinin ülkeler özelinde dağılımı.

Ülke	Üzerinde UDP Çalışan Sunucu Sayısı
Malta	0
Bosna	0
Lihtenştayn	0
Andorra	0
Danimarka	1
Avusturya	1
İzlanda	1
Ermenistan	1
Kuzey Makedonya	1
Arnavutluk	1
Karadağ	1
Lüksemburg	2
Estonya	3
Finlandiya	4
Slovenya	4
Belarus	4
Yunanistan	5
Hırvatistan	6
Belçika	6
Moldova	7
Slovakya	8
Sırbistan	10
Norveç	14
Portekiz	15
İrlanda	20
Bulgaristan	28
İsviçre	29
Letonya	30
İspanya	32
Macaristan	34
Çekya	41
İsveç	71
Romanya	78
Ukrayna	89
Polonya	96
İtalya	163
Litvanya	338
Fransa	347
Hollanda	385
Birleşik Krallık	401
Almanya	580
Türkiye	595
Rusya	786

Çizelge 4.9: Ülkeler özelinde memcached sunucusu başına düşen yükseltici sayısı.

Ülke	Memcached Sunucu Sayısı	Üzerinde UDP Çalışan Sunucu Sayısı	Sunucu Başına Düşen Yükseltici Sayısı
Andorra	1	0	0.0000000
Bosna	39	0	0.0000000
Lihtenştayn	2	0	0.0000000
Malta	40	0	0.0000000
Hırvatistan	64871	6	0.0000925
Danimarka	8703	1	0.0001149
Finlandiya	32500	4	0.0001231
Avusturya	3932	1	0.0002543
Belçika	13962	6	0.0004297
Estonya	4313	3	0.0006956
İzlanda	693	1	0.0014430
Norveç	9216	14	0.0015191
Hollanda	146677	385	0.0026248
Fransa	129797	347	0.0026734
Birleşik Krallık	146677	401	0.0027339
Romanya	26864	78	0.0029035
İspanya	8907	32	0.0035927
Letonya	8212	30	0.0036532
Polonya	25031	96	0.0038352
Slovenya	960	4	0.0041667
İtalya	27901	163	0.0058421
Yunanistan	698	5	0.0071633
Çekya	5290	41	0.0077505
İsveç	6557	71	0.0108281
Almanya	42658	580	0.0135965
İsviçre	2060	29	0.0140777
Lüksemburg	110	2	0.0181818
Ermenistan	47	1	0.0212766
K. Makedonya	46	1	0.0217391
Arnavutluk	35	1	0.0285714
Slovakya	242	8	0.0330579
Macaristan	770	34	0.0441558
Türkiye	11719	595	0.0507723
Bulgaristan	513	28	0.0545809
Portekiz	226	15	0.0663717
Ukrayna	1284	89	0.0693146
Rusya	9863	786	0.0796918
Sırbistan	115	10	0.0869565
Karadağ	11	1	0.0909091
Belarus	43	4	0.0930233
Moldova	70	7	0.1000000
İrlanda	185	20	0.1081081
Litvanya	430	338	0.7860465

Memcached sunucularının sıkılaştırılmasındaki en temel unsur; eğer mecburi bir durum yok ise sunucunun internet üzerinden yayın yapmamasıdır. Keşfedilen memcached sunucularının bu gereksinimleri sadece sunucuyu yöneten kişiler tarafından öngörülebileceği için ülkeler arası kıyaslamalar gerçekçi olmayabilir. Çalışma sonucunda kesin noktalar ise UPD port 11211 üzerinden yayın yapan sunucu sayıları ve bunların riskleridir. Memcached "status" bilgilerinin alınabildiği ve üzerinde UDP portunun çalıştığı sunucu sayıları göz önünde bulundurulduğu zaman; Rusya, Türkiye, Almanya, Birleşik Krallık, Hollanda ve Fransa' da keşfedilen yükseltici sayısı tüm kapsamın yaklaşık olarak %64' ünü sağlamaktadır.

4. SONUÇ VE ÖNERİLER

İnternet üzerinden verilen hizmetlerin çeşitliliğinin artması ile birlikte hizmet engelleme saldırıları ayrı bir boyut kazanmıştır. Saldırganlar mali olarak zarar vermek amacı ile ya da hizmet veren kurumların imajlarını zedelemek için hizmet engelleme saldırılarına başvurmaktadır. Servis yöneticileri öncelikli olarak kendi sistemlerine sızılmasına sebep olabilecek zafiyetleri kapatmaya meyillidir. Bu çalışmada DNS, NTP ve memcached sunucularında bulunan, sistemin ele geçirilmesine sebep olmamakla birlikte yönetilen sunucular üzerinden başkalarına zarar verebilecek açıklıkları, diğer bir deyiş ile dağıtık yansıtılmış hizmet engelleme saldırılarında yükseltici/yansıtıcı olarak kullanılabilme durumları 43 ülkede ele alınmıştır. Bu servislerin ülkeler özelinde geniş çaplı bir tarama ile keşfedilmelerinden sonra zafiyet barındırma durumları incelenmiştir. Bu zafiyetler ve ilgili çözümleri; DNS için 2006, NTP için 2013 ve memcached için 2018 de yayınlanmış olmasına karşın saldırganlar tarafından yükseltici olarak kullanılabilecek çok sayıda sunucu tespit edilmiştir. Sunucuların sıkılaştırılma oranları ülkelere göre büyük farklılıklar göstermektedir. Kapsam dâhilindeki üç protokol için, Estonya, Malta ve Hırvatistan gibi bazı ülkelerde gerek sıkılaştırma bilincinin gerek ise sıkılaştırma işlemi için gerekli aktiviteyi sağlayabilme kapasitesinin üst düzeyde olduğu görülmüştür. Lihtenştayn ve Danimarka güncelleme işlemi yapılarak sıkılaştırılabilinen NTP ve memcached servislerinde başarı gösterip, sadece el yordamı ile sıkılaştırma işlemi yapılabilen DNS servisinde bu başarıdan uzak kalması dikkat çeken bir husustur. Ermenistan, Arnavutluk, Macaristan ve Türkiye ise sıkılaştırma bilincinin eksikliği ile ön plana çıkan ülkelerdir. Özellikle NTP ve memcached sunucularının sıkılaştırılması çok basittir. DNS sunucularının ise bu zafiyetinin kapatılması biraz daha karmaşıktır. Otomatik olarak kapatılamayan DNS zafiyeti için iki temel sıkılaştırma unsuru vardır. Bunlardan ilki özyinelemeli sorguya izin verilmemesidir. Özyinelemeli sorgulara izin

verilmesi durumunda, cevap saldırı için yansıtıcı olarak kullanılacak ve sunucunun elinde olsun ya da olmasın sorgulanan DNS sunucusu alanı ile ilgili tüm bilgiyi öğrenip sorgu yapılan noktaya gönderilecektir [34].

Ayrıca özyinelemeli sorguların açık olması saldırıda aracı olarak kullanılacak sisteminde zarar görmesine sebep olabilecektir. Kendilerine düzenlenen bir saldırıda sürekli olarak başka sunucular ile irtibata geçmek kendi sistemlerini yoracaktır. Özyinelemeli sorguların nasıl kapatılacağı ile ilgili sayısız kaynak mevcuttur.

DNS sunucularının yansıtıcı olarak kullanılmasının önüne geçecek bir diğer önemli yöntem ise "ANY" sorgusunun kısıtlanması ve sadece yetkili kişiler ya da IP'ler tarafından yapılmasına izin verilmesidir. Böylece sıkılaştırma ile birlikte saldırganlar tarafından yönetilen botnetler bu sorguyu yapamayacakları için DNS sunucusu saldırıda anlamsız hale gelecektir [35].

Çalışma sırasında ele alınan ikinci protokol olan NTP nin en temel sıkılaştırma yöntemi: güncellemektir. 4.2.7'den önceki tüm ntpd sürümleri varsayılan olarak zafiyeti barındırmakta, yani "monlist" sorgulamasına açık ve herhangi birisi tarafından yapılmış "monlist" sorgusuna yanıt verebilmektedir. Sistemlerin güvenliği açısından en kritik unsurlardan olan, sistemlerin mümkün olduğu kadar en güncel halde tutulması konusu burada da kendini göstermektedir. NTP sunucularının sıkılaştırılması için elle işletilen yöntemler de mevcuttur. Bu yöntemlerdeki temel prensip "monlist" sorgusunu tamamen kapatmak ya da sadece belirli kişilerin yapabilmesini sağlamak üzerinedir [36, 37].

Çalışmalarda üçüncü olarak ele alınan memcached servisinin bazı özel durumları mevcuttur. Memcached servis yöneticileri öncelikli olarak sistemlerinin internet üzerinden yayın yapma durumlarını ele almalıdır. Eğer sistem için internet üzerinden yapılan yayın vazgeçilmez değil ise servisin internet yayını durdurulmalıdır. İnternet yayınının zorunlu olarak ele alındığı durumlarda ise en temel çözüm UDP port 11211 üzerinden çalışmanın engellenerek sistemin sadece TCP protokolü ile çalışmasını sağlamaktır. GitHub saldırısından sonra yayınlanan 1.5.6 versiyonu ile birlikte varsayılan port olarak yalnızca TCP 11211 kullanılmaktadır [38]. Öte yandan bu işlem elle işletilebilir şekilde de yapılabilmektedir [39].

KAYNAKLAR

[1] S. M. Specht, R. B. Lee., (2004) Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures. International Conference on Parallel and Distributed Computing (and Communications) Systems (ISCA PDCS), San Francisco, CA, ABD

[2] M. Kührer, T. Hupperich, C. Rossow, and T. Holz., (2014) Exit from Hell? Reducing the Impact of Amplification DDoS Attacks, 23. USENIX Security Symposium, San Diego, ABD

[3] C. Rossow., (2014)Amplification Hell: Revisiting Network Protocols for DDoS Abuse. Network and Distributed System Security (NDSS) Symposium

[4] Marc Kuhrer, Thomas Hupperich, Christian Rossow, Thorsten Holz., (2014) Hell of a Handshake: Abusing TCP for Reflective Amplification DDoS Attacks 23. USENIX Security Symposium, San Diego, ABD

[5]Üretici Yayını, 5 cyber security myths, the importance of time synchronization, and more Ocak 2010, https://www.eventtracker.com/blog/2010/january/5-cyber-security-myths-the-importance-of-time-synchronization/ Alındığı Tarih: 28.07.2019

[6] S. M. Bellovin., (1989) "Security Problems in the TCP/IP Protocol Suite," ACM SIGCOMM Comput. Commun. Rev., vol. 19, no. 2, pp. 32–48, Apr. 1989

[7] CERT Advisory, (2014) "UDP-Based Amplification Attacks" https://www.us-cert.gov/ncas/alerts/TA14-017A Alındığı Tarih 28.07.2019

[8] Prolexic Quarterly Global DDoS Attack Report Q2 2013, (2013) "Prolexic Stops Largest-Ever DNS Reflection DDoS Attack," https://sm.asisonline.org/ASIS%20SM%20Documents/Prolexic%20Quarterly%20Global%20DDoS%20Attack%20Report.pdf. Alındığı Tarih 28.07.2019

[9] F. J. Ryba, M. Orlinski, M W¨ahlisch, C. Rossow, T. C. Schmidt., (2016) "Amplification and DRDoS Attack Defense – A Survey and New Perspectives". arXiv:1505.07892v3 [cs.NI]

[10] T. Brewster, (2013) "Cyber Attacks Strike Zimbabweans Around Controversial Election,": http://www.techweekeurope.co.uk/workspace/ zimbabwe-election-cyber-attacks-123938 Alındığı Tarih 28.07.2019

[11]] Matthew Prince, (2013) The DDoS That Knocked Spamhaus Offline (And How We Mitigated It) https://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho/ Alındığı Tarih: 28.07.2019

[12] Matthew Prince, (2013) The DDoS That Almost Broke the Internet https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/ Alındığı Tarih: 28.07.2019

[13] Dean Takashi, (2013) Hackers attack Dota 2 and League of Legends servers in quest for one game livestreamer https://venturebeat.com/2013/12/30/hackers-attack-dota-2-and-league-of-legends-servers-in-quest-for-one-game-livestreamer/ Alındığı Tarih: 28.07.2019

[14] MITRE, (2018) National Vulnerability Database, "CVE-2006-0987 Detail " https://nvd.nist.gov/vuln/detail/CVE-2006-0987#vulnCurrentDescriptionTitle Alındığı Tarih: 28.07.2019

[15] MITRE, (2018) National Vulnerability Database, "CVE-2006-0988 Detail " https://nvd.nist.gov/vuln/detail/CVE-2006-0988#vulnCurrentDescriptionTitle Alındığı Tarih: 28.07.2019

[16] Nic.TR, (2015) 14/12/2015 Tarihinde Başlayan DDoS Saldırısı Kamuoyu Duyurusu. https://www.nic.tr/2015-12-DDoS-Saldirisi-Kamuoyu-Duyurusu-20151221.pdf . 21 Dec 2015 Alındığı Tarih: 28.07.2019

[17] S. Hilton., (2016) Dyn Analysis Summary Of Friday October 21 Attack https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/. Alındığı Tarih: 28.07.2019

[18] MITRE, (2018) National Vulnerability Database, "CVE-2006-0988 Detail" https://nvd.nist.gov/vuln/detail/CVE-2013-5211 Alındığı Tarih: 28.07.2019

[19] M. Prince. (2014) Technical Details Behind a 400 Gbps NTP Amplification DDoS Attack. https://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/ Alındığı Tarih: 28.07.2019

[20] What is Memcached? https://memcached.org/

[21] MITRE, (2018) National Vulnerability Database, "CVE-2018-100015 Detail https://nvd.nist.gov/vuln/detail/CVE-2018-1000115 Alındığı Tarih: 28.07.2019

[22] S. Kottle, (2018) February 28th DDoS Incident Report, https://githubengineering.com/ddos-incident-report/ Alındığı Tarih: 28.07.2019

[23] Carlos Morales., (2018) NETSCOUT Arbor Confirms 1.7 Tbps DDoS Attack; The Terabit Attack Era Is Upon Us, https://www.netscout.com/blog/asert/netscout-arbor-confirms-17-tbps-ddos-attack-terabit-attack-era Alındığı Tarih: 28.07.2019

[24] Common Vulnerability Scoring System Calculator Version 2 https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator / Alındığı Tarih: 28.07.2019

[25] Common Vulnerability Scoring System Calculator Version 3 https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator / Alındığı Tarih: 28.07.2019

[26] I. Erben., (2014) Generating country IP ranges lists http://blog.erben.sk/2014/01/28/generating-country-ip-ranges-lists/ Alındığı Tarih: 28.07.2019

[27] I. Erben. http://www.iwik.org/ipcountry/ Alındığı Tarih: 28.07.2019

[28] Z. Durumeric, E. Wustrow, and J. A. Halderman., (2013) ZMap: Fast Internet-wide Scanning and Its Security Applications. In Proceedings of the 22. USENIX Security Sempozyumu, Washington, D.C., ABD

[29] The ZMap Project https://zmap.io/ Alındığı Tarih: 28.07.2019

[30] E. M. Ercan, A.A. Selcuk., (2018) A Nationwide Study of DRDoS Amplifiers, ISC Turkey, Ankara, Türkiye

[31] E. M. Ercan, A.A. Selcuk., (2018) An Analysis DRDoS Amplifiers in Europe, ICONCS 2018, Karabük, Türkiye

[32] Zmap UDP Probes Examples https://github.com/zmap/zmap/blob/master/examples/udp-probes/README Alındığı Tarih: 28.07.2019

[33] https://nmap.org/ Alındığı Tarih: 28.07.2019

[34] CERT Advisory, "DNS Amplification Attacks" https://www.us-cert.gov/ncas/alerts/TA13-088A Alındığı Tarih: 29.07.2019

[35] Use DNS Policy for Applying Filters on DNS Queries. (2019) https://docs.microsoft.com/en-us/windows-server/networking/dns/deploy/apply-filters-on-dns-queries, Alındığı Tarih: 29.07.2019

[36] J. Graham-Cumming. (2014) Understanding and Mitigating NTP-Based DdoS Attacks. https://blog.cloudflare.com/understanding-and-mitigating-ntp-based-ddos-attacks/ , Alındığı Tarih: 29.07.2019

[37] Team Cymru. Secure NTP Template. https://www.team-cymru.com/secure-ntp-template.html Alındığı Tarih: 29.07.2019

[38]Dormando,(2018),https://github.com/memcached/memcached/wiki/ReleaseNotes156 Alındığı Tarih: 29.07.2019

[39] Alibaba Cloud, (2018) Harden Memcached service security https://www.alibabacloud.com/help/faq-detail/37553.htm Alındığı Tarih: 29.07.2019

EKLER

EK 1: Zmap ile DNS sunucularının keşfedilmesi

```
#!/bin/sh

END=6

x=$END

while [ $x -gt 0 ];

do

sleep 1

zmap -p 53 -M udp -w [Girdi Listesi Yolu]/[Girdi Listesi] -c 20 --ignore-invalid-
hosts -B 15M >> [Çıktı Listesi Yolu]/[Çıktı Listesi İsmi]

sleep 1

zmap -p 53 -M udp --probe-args=file[Sorgu Paketinin Bulunduğu
Yol]/dns_53_queryAwww.google.it.pkt -w [Girdi Listesi Yolu]/[Girdi Listesi] -c 20
--ignore-invalid-hosts -B 15M >> [Çıktı Listesi Yolu]/[Çıktı Listesi İsmi]

sleep 1

zmap -p 53 --probe-args=file:[Sorgu Paketinin Bulunduğu
Yol]/dns_53_queryAwww.google.com.pkt w [Girdi Listesi Yolu]/[Girdi Listesi] -c
20 --ignore-invalid-hosts -B 15M >> [Çıktı Listesi Yolu]/[Çıktı Listesi İsmi]

 x=$(($x-1))

done
```

EK 2: DNS Sorguları İçin Hazırlanan Kod Parçacığı

```
#!/bin/sh
for LINE in `cat [zmap çıktı dosyasının ismi]`
do
  echo "-----------------------------------------" >> [script sonuçlarının yazılacağı dosya]
  echo "IP = $LINE\n" >> [script sonuçlarının yazılacağı dosya]
  nslookup -q=ANY www.etu.edu.tr $LINE >> [script sonuçlarının yazılacağı dosya]

done
```

EK 3: Zmap ile NTP Sunucularının Keşfedilmesi

zmap -M ntp -p 123 --max-sendto-failures 10000000 --bandwidth=15M --whitelist-file=[Girdi Listesi Yolu]/[Girdi Listesi] >> [Çıktı Listesi Yolu]/[Çıktı Listesi İsmi]

EK 4: Nmap ile “monlist” sorgusunun yapılması

nmap -sU -n -p 123 -Pn --script=ntp-monlist -iL [zmap çıktı listesi yolu]/[zmap çıktısı] -oN /[nmap çıktı listesi yolu]/[nmap çıktısı]

EK 5: Zmap ile memcached Sunucularının Keşfedilmesi

zmap -p 11211 --probes=1 --probe-args=file: Sorgu Paketinin Bulunduğu Yol]/memcache_11211.pkt --ignore-invalid-hosts --whitelist-file= [Girdi Listesi Yolu]/[Girdi Listesi] -B 15M >> [Çıktı Listesi Yolu]/[Çıktı Listesi İsmi]

EK 6: Nmap ile zafiyetli memcached sunucularının keşfi

nmap -p 11211 --script memcached-info -iL [zmap çıktı listesi yolu]/[zmap çıktısı] -oN /[nmap çıktı listesi yolu]/[nmap çıktısı]

ÖZGEÇMİŞ

Ad-Soyad **:**Emre Murat ERCAN

Uyruğu **:**T.C.

Doğum Tarihi ve Yeri **:** 18.12.1990 / Ankara

E-posta **:**emremuratercan@yandex.com

ÖĞRENİM DURUMU:

- **Lisans** **:** 2015, TOBB Ekonomi ve Teknoloji Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği
- **Yükseklisans** **:** 2019, TOBB Ekonomi ve Teknoloji Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği, Bilgi Bilgi Güvenliği

MESLEKİ DENEYİM VE ÖDÜLLER:

Yıl	Yer	Görev
2017 –	Barikat İnternet Güvenliği	Bilgi Güvenliği Danışmanı
2017 – 2017	Pi Kalite ve Danışmanlık	Bilgi Güvenliği Danışmanı

YABANCI DİL:

İngilizce

TEZDEN TÜRETİLEN YAYINLAR, SUNUMLAR VE PATENTLER:

- **E. M. Ercan, A.A. Selcuk.,** (2018) A Nationwide Study of DRDoS Amplifiers, ISC Turkey, Ankara, Türkiye
- **E. M. Ercan, A.A. Selcuk.,** (2018) An Analysis DRDoS Amplifiers in Europe, ICONCS 2018, Karabük, Türkiye