AKTİF SİBER SAVUNMA TEKNİKLERİ
VE
PERFORMANS ANALİZİ

YÜKSEK LİSANS TEZİ

Recep ÖZBAY

DANIŞMAN
Yrd. Doç. Dr. Uğur FİDAN

II. DANIŞMAN
Uzm. Emin ÇALIŞKAN

İNT. VE BİL. TEK. YÖN. ANABİLİM DALI

Aralık, 2015

AFYON KOCATEPE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

AKTİF SİBER SAVUNMA TEKNİKLERİ VE PERFORMANS ANALİZİ

Recep ÖZBAY

I. DANIŞMAN
Yrd. Doç. Dr. Uğur FİDAN
II. DANIŞMAN
Uzm. Emin ÇALIŞKAN

İNTERNET VE BİLİŞİM TEKNOLOJİLERİ YÖNETİMİ
ANABİLİM DALI

ARALIK, 2015

TEZ ONAY SAYFASI

Recep ÖZBAY tarafından hazırlanan "Aktif Siber Savunma Teknikleri Ve Performans Analizi" adlı tez çalışması lisansüstü eğitim ve öğretim yönetmeliğinin ilgili maddeleri uyarınca 17/12/2015 tarihinde aşağıdaki jüri tarafından oy birliği ile Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü İnternet ve Bilişim Teknolojileri Yönetimi **Anabilim Dalı'nda YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman : Yrd. Doç. Dr. Uğur FİDAN

İkinci Danışman : Uzm. Emin ÇALIŞKAN

Başkan : Yrd. Doç. Dr. Süleyman A. SULAK
Necmettin Erbakan Üniversitesi
Ahmet Keleşoğlu Eğitim Fakültesi

Üye : Yrd. Doç. Dr. Ertuğrul ERGÜN
Afyon Kocatepe Üniversitesi
Uzaktan Eğitim Meslek Yüksek Okulu

Üye : Yrd. Doç. Dr. Uğur FİDAN
Afyon Kocatepe Üniversitesi Mühendislik Fakültesi

Afyon Kocatepe Üniversitesi
Fen Bilimleri Enstitüsü Yönetim Kurulu'nun
...../...../..... tarih ve
……. sayılı kararıyla onaylanmıştır.

…….
Prof. Dr. Hüseyin ENGİNAR
Enstitü Müdürü

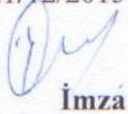
BİLİMSEL ETİK BİLDİRİM SAYFASI
Afyon Kocatepe Üniversitesi

Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- Görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- Başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- Atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- Kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- Ve bu tezin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

21/12/2015



İmza

Recep ÖZBAY

ÖZET
Yüksek Lisans Tezi

AKTİF SİBER SAVUNMA TEKNİKLERİ VE PERFORMANS ANALİZİ

Recep ÖZBAY
Afyon Kocatepe Üniversitesi
Fen Bilimleri Enstitüsü
İnternet ve Bilişim Teknolojileri Yönetimi Anabilim Dalı
Danışman: Yrd. Doç. Dr. Uğur FİDAN
II. Danışman: Uzm. Emin ÇALIŞKAN

Bu çalışmada, bilişim sistemlerinin kullanım alanlarının ve buna bağlı olarak öneminin artışı ile doğru orantılı olarak artan ve gelişen siber saldırılar üzerinde çalışılmıştır. Siber ölüm zinciri kapsamında gelişmiş siber saldırıların (advanced persistent threat - APT) aşamaları incelenmiştir. Gelişmiş siber saldırılara örnekler verilmiştir. Ayrıca, gelişmiş siber saldırılar karşısında yetersiz kalan geleneksel güvenlik çözümlerine ilave olarak aktif siber savunma yöntemlerinin kullanılabileceği literatürdeki çalışmalardan da faydalanılarak savunulmuştur. Aktif siber savunma kapsamında, aldatma, yavaşlatma ve karşı atak tekniklerinin kullanılabileceği anlatılmıştır. Proje kapsamında kurulan laboratuvar ortamında, aktif siber savunmanın karşı atak ve yavaşlatma etkileri gösterilmeye çalışılmıştır. Ayrıca, aktif siber savunmaya yönelik araçlarla donatılmış Aktif Savunma Harbinger Dağıtımı (Active Defense Harbinger Distribution - ADHD) sanal makinesinin aktif siber savunmada nasıl kullanılabileceğine dair örnekler laboratuvar ortamında gösterilmeye çalışılmıştır. Laboratuvar ortamında yapılan deneylerin siber saldırılar karşısında pozitif etkileri olduğu gözlemlenmiştir. Sonuç olarak, aktif siber savunma tekniklerinin ulusal güvenliği artırmak için, kamu kurumlarında nasıl kullanılabileceği belirtilmiştir. Aktif siber savunmanın uygulanmasındaki hukuki kısıtlamalar verilmiştir.

2015, x + 55 sayfa
Anahtar Kelimeler: Aktif Siber Savunma, Siber Güvenlik, Siber Ölüm Zinciri

ABSTRACT
M.Sc Thesis

ACTIVE CYBER DEFENSE TECHNIQUES AND PERFORMANCE ANALYSIS

Recep ÖZBAY
Afyon Kocatepe University
Graduate School of Natural and Applied Sciences
Department of Internet and Information Technology Management
Supervisor: Asst. Prof. Uğur FİDAN
Co-Supervisor: Expert Emin ÇALIŞKAN

In this study, cyber-attacks that it increases in direct proportion with the areas of information systems and depending on their importance have been studied. Phases of advanced persistent threat (APT) have been examined within cyber kill chain. Examples of advanced persistent threat are given. Moreover, the idea that active cyber defense methods can be used in addition to traditional security solutions that have been inadequate against to APT has been advocated under cover of literature. Deception, slow down and counter attack techniques can be used within the scope of active cyber defense, has explained. To show counter attack and slow down effects of active cyber defense in the laboratory was established in project has tried. In addition, examples of Active Defense Harbinger Distribution (ADHD) virtual machine, equipped with tools for active cyber defense, how to use for active defense have attempted in laboratory. Positive effects of the experiments conducted in the laboratory against to cyber-attacks has been observed. As a result, active cyber defense techniques how it can be used in public institutions to improve national security has been discussed. Legal risks of implementation of active cyber defense has been mentioned.

2015, x + 55 pages

Keywords: Active Cyber Defense, Cyber Security, Cyber Kill Chain

TEŞEKKÜR

Bu araştırmanın konusu, deneysel çalışmaların yönlendirilmesi, sonuçların değerlendirilmesi ve yazımı aşamasında yapmış olduğu büyük katkılarından dolayı tez danışmanım Sayın Yrd. Doç. Dr. Uğur Fidan'a, akademik ve teknik desteklerinden sonra ayrıca tıkandığım noktalarda beni motive ederek ve çıkış yolları göstererek manevi destekte de bulunan ikinci danışmanım Sayın Uzm. Emin Çalışkan'a, her konuda öneri ve eleştirileriyle yardımlarını gördüğüm hocalarıma ve arkadaşlarıma teşekkür ederim.

Bu araştırma boyunca maddi ve manevi desteklerini esirgemeyen aileme teşekkür ederim.

Recep ÖZBAY

AFYONKARAHİSAR, 2015

İÇİNDEKİLER DİZİNİ

Sayfa

ÖZET iii
ABSTRACT iv
TEŞEKKÜR v
İÇİNDEKİLER DİZİNİ vi
KISALTMALAR DİZİNİ viii
ŞEKİLLER DİZİNİ ix
1. GİRİŞ 1
2. LİTERATÜR BİLGİLERİ 3
3. MATERYAL 6
3.1 Gelişmiş Siber Saldırı (Advanced Persistent Threat - APT) 6
3.1.1 Siber Ölüm Zinciri 7
3.1.2 Yaşanmış APT Saldırılarından Örnekler 8
3.1.2.1 APT1 9
3.1.2.2 APT30 12
3.1.2.3 Shady RAT 13
3.2 Aktif Siber Savunma (Active Cyber Defense - ACD) 13
3.2.1 Balküpü (Honeypot) 15
3.2.2 Dünyada Aktif Siber Savunmaya Bakış ve Örnekler 18
3.2.3 Aktif Siber Savunma Tekniklerinin Uygulamasında Hukuki Kısıtlamalar 20
3.3 Kamu Kurumlarında Siber Savunma ve Eksiklikler 22
4. METOT 25
4.1 Aktif Siber Savunma Teknikleri 25
4.2 Aktif Siber Savunmanın Siber Ölüm Zincirinde Yeri ve Etkileri 26
4.3 ACD Yöntemlerinin Siber Saldırılara Karşı Etkisinin İncelenmesi 27
4.3.1 DOS ve DDOS Saldırılarının Karşı Atak Etkisinin İncelenmesi 28
4.3.1.1 DOS ve DDOS Testi Senaryosu 29
4.3.2 Active Defense Harbinger Distribution'nin (ADHD) Aktif Siber Savunmada Kullanılması 31
4.3.2.1 Saldırganlar Hakkında Bilgi Toplama Test Senaryosu 32
4.3.2.2 Saldırganı Yavaşlatma Test Senaryosu 33
4.3.2.3 Karşı Atak Test Senaryosu 34

5. BULGULAR 36
5.1 DOS ve DDOS Testi Sonucu 36
5.2 Saldırganlar Hakkında Bilgi Toplama Testi Sonucu 39
5.3 Saldırganı Yavaşlatma Testi Sonucu 41
5.4 Karşı Atak Testi Sonucu 45
6. TARTIŞMA 48
7. KAYNAKLAR 51
ÖZGEÇMİŞ 55

KISALTMALAR DİZİNİ

Kısaltmalar	
ACD	Active cyber defense (Aktif siber savunma)
ADHD	Active Defense Harbinger Distribution (Aktif Savunma Harbinger Dağıtımı)
APT	Advanced persistent threat (Gelişmiş siber saldırı)
BeEF	The Browser Exploitation Framework Project (Tarayıcı Sömürme Çerçeve Projesi)
DDOS	Distributed Denial of Service (Dağıtık Servis Dışı Bırakma)
DMZ	Demilitarized zone-Sivil bölge
DNS	Domain name system (Alan adı sistemi)
DOS	Denial of Service (Servis Dışı Bırakma)
ENISA	European Union Agency for Network and Information Security
IDS	Intrusion detection system (Saldırı tespit sistemi)
IP	Internet protocol (İnternet protokolü)
IPS	Intrusion prevention system (Saldırı önleme sistemi)
Nmap	Network Mapper (ağ tarama ağacı)
SSH	Secure shell (Güvenli veri iletim ağ protokolü)
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
VOIP	Voice over intenet protocol (IP üzerinden ses haberleşme protokolü)

ŞEKİLLER DİZİNİ

Sayfa

Şekil 3.1 APT1'nın sızdığı ülkeler (İnt.Kyn.4) 9

Şekil 3.2 Sektörlere göre APT1'nın sızdığı firma sayısı (İnt.Kyn.4) 10

Şekil 3.3 Mandiant'ın saldırı yaşam zinciri modeli (İnt.Kyn.4) 11

Şekil 3.4 Doğrulanmış APT1 sunucularının ülkelere göre dağılımı (İnt.Kyn.4) 12

Şekil 3.5 Balküplerinin sınıflandırılması (Grudziecki *et al.* 2012) 15

Şekil 4.1 Karşı atak denemelerinde kullanılan laboratuvarın ağ yapısı 29

Şekil 4.2 Hping3 aracı ile DOS saldırısı yapma 20

Şekil 4.3 Hping3 aracı ile DDOS saldırısı yapma 31

Şekil 4.4 Testin ikinci aşamasında kullanılan ağ topolojisi 31

Şekil 4.5 Honey Badger tarafından cevap olarak verilen HTML kodu 32

Şekil 4.6 Tüm portların 4444 portuna yönlendirilmesi 34

Şekil 4.7 Birinci tarama 34

Şekil 4.8 İkinci tarama 34

Şekil 4.9 BeEF aracı üzerindeki saldırı modülleri 35

Şekil 5.1 Test ortamında DOS saldırısı esnasında ulaşılan bant genişliği 36

Şekil 5.2 Test ortamında DDOS saldırı esnasında ulaşılan bant genişliği 36

Şekil 5.3 Gerçek ortamda DOS saldırısı esnasında ulaşılan bant genişliği 37

Şekil 5.4 Gerçek ortamda DDOS saldırı esnasında ulaşılan bant genişliği 37

Şekil 5.5 Gerçek bir saldırıda isteklere cevap veremez hale gelmiş sunucu 38

Şekil 5.6 Saldırganın konum paylaşma isteğine olumlu cevap vermesi ile elde edilen bilgiler 39

Şekil 5.7 Saldırganın javascript kodu çalıştırılması isteğine olumlu cevap vermesi ile elde edilen bilgiler 40

Şekil 5.8 Saldırganların harita üzerinde konumlarının gösterilmesi 41

Şekil 5.9 Spidertrap uygulaması kapalıyken yapılan taramanın sonucu 42

Şekil 5.10 Spidertrap uygulaması açıkken yapılan taramanın sonucu 42

Şekil 5.11 Portspoof aracı kapalıyken yapılan taramanın sonucu 43

Şekil 5.12 Portspoof aracı açıkken yapılan tarama sonucu 43

Şekil 5.13 Portspoof aracı kapalıyken yapılan taramanın sonucu 44

Şekil 5.14 Portspoof aracı açıkken yapılan tarama sonucu 44

Şekil 5.15 Saldırganın tarayıcısı hakkında bilgiler 46

Şekil 5.16 Saldırganın makinesi hakkında bilgiler 46

Şekil 5.17 Saldırgan makineye yönelik port taraması 47

1. GİRİŞ

Bilgi ve iletişim sistemleri her geçen gün daha fazla kullanılmaları ile birlikte, bu sistemlerin güvenliğinin sağlanması hem ulusal güvenliğin, hem de rekabet gücünün önemli bir boyutu haline gelmiştir. Bilgi ve iletişim sistemlerinde bulunan güvenlik zafiyetleri, bu sistemlerin hizmet dışı kalmasına veya kötüye kullanılmasına, can kaybına, büyük ölçekli ekonomik zarara, kamu düzeninin bozulmasına ve/veya ulusal güvenliğin ihlaline neden olmaktadır (Resmi Gazete 2013). Siber saldırılar ve siber güvenliğin önemi, bilişim sistemlerinin insan hayatındaki yeri arttıkça yani IP (internet protokolü) adresi alan cihazların sayısı arttıkça, her geçen gün artmaktadır.

Saldırılarda potansiyel kazanç olduğu sürece, bilgisayar korsanları sistemlere saldırmaya devam edecekler ve kişisel şöhret ya da sistemleri ele geçirme heyecanı algılanan riski artıracaktır. (Anderson *et al.* 2005). Günümüzde birçok bilgi sistemi ülkeler açısından kritik bilgiler barındırmaktadır. Bu kritik bilgilerin güvenlik zafiyetlerinden ötürü siber teröristler tarafından kötüye kullanılması durumunda ülkeler açısından felaketler meydana gelmektedir (Vural *et al.* 2009).

Saldırıların çalınan maldan idari para cezalarına, yasal zararlardan maddi tazminata kadar önemli maddi zararları beraberinde getirmekte olduğu görülmüştür. Ancak bu buzdağının sadece görünen kısmıdır. Asıl önemli zararlar başta rekabet avantajının kaybedilmesi, müşterinin güveninin kaybedilmesi, kurumun itibarının ve markasının zedelenmesi olmak üzere maddi olmayan varlıklarda görülmektedir. Bu gibi maddi olmayan varlıklar kurumun stratejik pazar konumu ve hisse fiyatları üzerinde önemli bir etkiye sahip olabilmektedir (İnt.Kyn.2).

İngiliz hükümeti, çoğunlukla siber casusluk ve fikri mülkiyet hırsızlığından kaynaklı siber suçların 2011'de ekonomisine maliyetinin yaklaşık 44 milyon dolar olduğunu ya da bir diğer ifadeyle İngiliz yurt içi gayri safi milli hasılanın %2'sine eşit olduğunu tahmin etmektedir (Lachow 2013). Ulusal bilgi sistemlerinin ortak olarak kullanılmaya başlanmasıyla, bilgi sistemlerinde muhafaza edilen ve ülke güvenliği açısından kritik olan bilgilerin güvenliğinin yüksek seviyede sağlanması anayurt güvenliği açısından önem kazanmıştır (Vural *et al.* 2009).

Aktif siber savunma konsepti ele alındığında birden fazla, yöntem, teknik veya yaklaşım ortaya çıkmaktadır. Güvenlik uzmanları gelişmiş siber saldırıları tamamen durdurmanın çok mümkün olmadığının farkındadırlar. Bundan dolayı da zararı aza indirecek yöntemler geliştirmeye çalışmaktadırlar. Bu çabalar bazen aldatma, bazen yavaşlatma, bazen şaşırtmaca bazen karşı atak yaparak düşmanı engelleme ya da tamamen yok etme olarak ortaya çıkmaktadır. Bundan dolayı da savunmayı güçlü kılmak adına farklı metotlar öne sürülmektedir. Adından da anlaşılacağı üzere, aktif siber savunmanın dinamik bir savunma yaklaşımı olduğu görülür. Bu çalışmaların ortak yanı konunun hukuki yönlerinden ziyade işin teknik tarafına odaklanmış olmalarıdır.

Gelişmiş siber saldırı yapan saldırganlar geleneksel savunma sistemlerine yakalanmamak ve hedeflerine ulaşmak için zorlu birkaç adımı atlatmak zorundadırlar. Lockheed Martin Şirketinin güvenlik uzmanları da bu saldırıyı daha iyi analiz edebilmek ve cevap verebilmek için bu saldırı türünü yedi faza ayırmışlardır (Hutchins *et al.* 2011). Bu çalışmanın kapsamında pasif savunma sistemlerini etkisiz hale getirebilen gelişmiş siber saldırı yöntemlerinin araştırılması, bu saldırı yöntemlerinin aşamaları (siber ölüm zinciri) ve yaşanmış örneklerin araştırılması vardır. Ayrıca bu saldırı yöntemlerine karşı kullanılmak üzere geliştirilen aktif siber savunma yöntemlerinin araştırılması, bu kapsamda yapılan çalışmaların araştırılarak aktif siber savunma yönteminin saldırılar karşısındaki etkinliğinin ölçülmesi de bu çalışmanın kapsamındadır.

Bu çalışmanın amacı, günümüzde artan ve daha karmaşık hale gelen siber saldırıları incelemek, pasif siber savunma (güvenlik duvarı, güncelleme takibi vb.) yöntemlerinden ziyade aktif siber savunma yöntemlerinin incelenmesi ve bunların ulusal güvenliği artırmak amacıyla nasıl kullanılabileceğini araştırmaktır.

2. LİTERATÜR BİLGİLERİ

2002-2015 tarihleri arasında konu ile ilgili yapılmış ulusal ve uluslararası literatür araştırması sonucunda 13 adet ulusal makale, 25 adet uluslararası makale, 6 adet ulusal rapor, 10 adet uluslararası rapor ve 20 adet internet kaynağı incelenmiştir. Sonrasında aktif siber savunma konsepti içine girebilecek çalışmalar aşağıda paylaşılmıştır.

Bir yazılımı üretenler tarafından bilinmeyen ve üreticileri bu açıklığın farkına varıp açıklığı kapatmadan önce bilgisayar korsanları tarafından sömürülen açıklıklar sıfırıncı gün (zero day) açıklığı olarak adlandırılır (İnt.Kyn.16). Gelişmiş siber saldırıların normal siber saldırılardan bir farkı da sıfırıncı gün açıklığı, olarak adlandırılan zararlı yazılımlar kullanılması olduğu söylenebilir.

Sıfırıncı gün açıklığı saldırıları gibi önceden bilinmeyen zararlı network hareketlerini saldırı tespit sistemleri (intrusion detection system - IDS) tespit edemezler. Vaarandi (2013) tarafından yapılan çalışmada insanların yazdığı imza veri tabanına güvenmek yerine ağ trafiğini normal ve anormal olarak sınıflandırmak için çeşitli algoritmalar kullanan ağ izleme yöntemleri önerilmiştir.

Anderson vd. (2005) yaptıkları çalışmada, geleneksel güvenlik tekniklerinin ağırlıklı olarak güvenlik duvarları, anti-virüsler, anti-casus yazılımları ve saldırı tespit sistemlerini kapsayan savunmaya dayalı (defansif-pasif) yaklaşıma dayandığını belirtmişlerdir.

Literatürde yer alan bir başka çalışma Lachow (2013) tarafından yapılmıştır. Bu çalışmada, saldırı sonrası algılama ve uyarı kullanan pasif savunma sistemlerine güvenmenin yetersiz olduğu belirtilmiştir. Ayrıca pasif savunma sistemlerini etkisiz hale getirebilen gelişmiş siber saldırılara karşı aktif siber savunma (active cyber defense -ACD) tekniklerinin kullanılmasını önermiştir. Lachow bunlara ilave olarak aldatmanın sadece saldırı için değil savunmayı güçlendirmek için saldırgana karşı kullanılabileceğini de ifade etmiştir.

Johnson ve Northcutt (2013) yaptıkları çalışmada aktif savunma sistemi kapsamında

aktif aldatma tekniklerinin organizasyonların güvenliğine önemli değer katacağını belirtmişler. Bu yaklaşımın temelinde saldırganın kıymetli ve hassas bilgiye erişebilmesi için gereken çabayı artırmak olduğunu ifade etmişler. Buna ilaveten eğer saldırganın sistem üzerinde harcadığı zaman ve kaynak artırılabilirse, saldırgan hakkında daha fazla bilgi toplanabileceğini belirtmişler.

Pingree vd. (2013) hiçbir tekil teknolojinin gelişmiş hedefli bir siber saldırıyı durduramayacağını savunmuşlar ve bu soruna çözüm olarak kapsamlı bir yaklaşım kullanılması gerektiğini belirtmişlerdir. Ayrıca bu çalışmada, saldırganların, sosyal mühendislik için dış kaynaklardan nasıl bilgi topladığı, bunları çalışanların güvenini kazanmak için nasıl kullandığı, e-posta ya da web sitesi gibi tüm iletişim yollarında oluşabilen şüpheli durumların önemi konusunda çalışanların bilinçlendirilmesi önerilmiştir.

Orans ve D'Hoinne tarafından (2013) yapılan çalışmada gelişmiş siber saldırılara karşı gelen ve giden network trafiğini analiz ederek tehlikeli bitiş noktalarının vurgulanabileceği, bu tekniğin avantajının son nokta ajanı gerektirmemesi olduğu ve bu yaklaşımın tüm son nokta ve işletim sistemleri için tespit etme imkânı sağladığı belirtilmiştir.

Anderson vd. (2005) tarafından yapılan çalışmada gelişmiş siber saldırılara cevap olarak aktif savunma teknolojilerinin en son aşırı noktasında, saldırganı yok etmek ya da ekonomik zarar vermek için saldırganların sistemlerine karşı saldırı olarak DDOS (distrubuted denial of servis - dağıtık servis dışı bırakma) saldırısı önerilmiştir. Ayrıca küçük ölçekli tarayıcı temelli servis dışı bırakma saldırılarının (DOS - denial of servis) tarayıcıdaki açıklığı sömürmek için zararlı kod göndererek bertaraf edilebileceği belirtilmiştir.

Isoda (2014) yaptığı çalışmada kıdemli güvenlik uzmanlarının derinlemesine savunma yaklaşımında sanayi, uzlaşma, pazarlama ve mesajlaşma eksikliklerinden dolayı sorunlarla karşı karşıya olduklarına değinmiştir. Bu stratejilerle daha iyi iletişim kurulmasına yardımcı olmak ve gelişmiş hedefli saldırılarla başa çıkmak için Japon kale

tasarım tekniklerinden faydalanılabileceğini belirtmiştir.

Literatürdeki bir başka çalışma Repik (2008) tarafından yapılmıştır. Bu çalışmada gelişmiş siber saldırılara karşı adres atlamanın (address hopping) keşif taramalarını ve ağ haritası çıkarmanın etkisini azaltacağı ve saldırganın sızma çalışmalarının yakalanma olasılığını artıracağı belirtilmiştir.

Zhuang vd. (2012) yaptıkları çalışmada siber saldılar karşısında ağ yapılandırmasının iki nedenden dolayı saldırı başarısını etkileyeceğini belirtmişlerdir. Bu iki nedeni;

- Saldırgan, ağ topolojisini çıkarmak için çok fazla zaman harcayacaktır (fiziksel ve mantıksal) ve bu diğer saldırılar için de faydalı olacaktır.
- Saldırgan elde ettiği sistemsel yetkileri uzun süre elinde tutamayacaktır ve tekrar tekrar sistemsel yetki elde etmek zorunda kalacaktır.

şeklinde açıklamışlardır.

Duszynski tarafından (İnt.Kyn.11) yapılan çalışmada gelişmiş siber saldırıların büyük çoğunluğunun aldatma üzerine kurulabileceği belirtilmiştir. Yani kullanıcıları aldatıp virüslü dosyayı açtırmak ya da zararlı bir siteyi ziyaret etmesini sağlamak gibi olduğu ifade edilmiştir. Aldatma sadece saldırı amaçlı operasyonlar için bir araç değil bunun yanı sıra bilgisayar savunmasını güçlendirmek için de kullanılabileceği belirtilmiştir. Siber aldatma yöntemiyle ve saldırganların yanlış ya da eksik bilgi içeren dokümanları çalmasına izin vererek fikri mülkiyet haklarının korunabileceği savunulmuştur.

Deloitte (İnt.Kyn.2) tarafından yayınlanan raporda, bir kurumun %100 güvenli olması mümkün olmasa da, üç temel özelliğe odaklanmak suretiyle siber tehditleri etkilerini azaltarak ve potansiyel iş zararını en aza indirerek yönetmesinin kesinlikle mümkün olacağı belirtilmiştir. Ayrıca iyi dengelenmiş bir siber savunmanın güvenli, farkında ve dirençli olması gerektiği belirtilmiştir.

3. MATERYAL

Bu bölümde gelişmiş siber saldırının (advanced persistent threat - APT) tanımına, siber ölüm zinciri yaklaşımı ile APT'nin aşamalarının neler olduğuna değinilecektir. Ayrıca yaşanmış APT saldırılarına örnekler verilecektir. Daha sonra APT'lere karşı çözüm olarak önerilen "Aktif siber savunma nedir ve hangi aşamalardan oluşur? Hangi yöntemler kullanılır? soruları ele alınacaktır. Aktif siber savunma konsepti içinde farklı amaçlar ile kullanılan bal küpleri (honeypot) ve çeşitleri belirtilecektir. Son olarak ise aktif siber savunmanın hukuki boyutu irdelenecektir.

3.1 Gelişmiş Siber Saldırı (Advanced Persistent Threat - APT)

Güvenlik uzmanları ile bilgisayar korsanları arasında devam eden mücadeleler sayesinde sistemlerin daha da güvenli hale geldiği savunulabilir. Bu yarışın sonucu olarak da ortaya gelişmiş siber saldırı olarak adlandırılan, çok daha karışık ve gelişmiş tekniklerin kullanıldığı ve uzun çalışmalar sonucunda ve belirli bir amaç doğrultusunda tecrübeli bilgisayar korsanları tarafından yapılan hatta devletlerin desteklediği bilinen ve/veya düşünülen saldırılar ortaya çıkmıştır. Bu gelişmiş saldırı türü APT (Advanced Persistent Threat) olarak adlandırılmıştır.

Genç bilgisayar korsanları ve küçük ölçekli suçlulardan ziyade karmaşık (sofistike) saldırı yapabilen tecrübeli bilgisayar korsanları ve devlet destekli saldırganlar devletler ve işletmeler için en çok tehlike arz eden tehditlerdir. Bu saldırganlar öncelikle kurumlardaki bilgileri çalmaya ve bireyleri ya da işletmeleri dolandırmaya odaklanmaktadır. APT saldırısı, genellikle devlet destekli olup gelişmiş yöntemlerle organizasyonlara sızarak haftalarca, aylarca hatta yıllarca bu organizasyonların tespit etmesine karşı saklanarak, bilgi kaçırmak için yapılan saldırıdır (Lachow 2013).

APT hedefi net olarak belirlenmiş, ileri seviyede ve uzun süreli tehditler içeren, siber savaşlarda kullanılmak üzere geliştirilmiş zararlı saldırı yazılımlarıdır. APT'ler genellikle devletlerin kritik altyapılarını hedeflemektedir (Kara 2013).

APT'ler siber savunma sistemlerini kolaylıkla atlatabilir ve yayılabilir. Gelişmiş

teknikler sayesinde hedef sisteme sızar ve bulaştığı sistemlerde uzun süre fark edilmeden çalışabilir. Sisteme kalıcı olarak yerleşir ve bilgi çalma, sistemi çökertme gibi hedeflerin yerine getirilmesini sağlar (Kara, 2013). APT mevcut çevre ve son nokta savunmasını aşmak için inşa edilmiş yeni saldırı doktrinidir (Lachow 2013).

Devlet destekli saldırılar genellikle inkâr edilse de, hedef ülkenin siber ortamına müdahale etmek, ekonomik zarar vermek ve istihbari bilgilerini ele geçirmek amaçlanmaktadır. Siber ortamda yaşanılan saldırılarla genellikle zarar vermek amaçlanmıştır ve ulusal bir güvenlik sorunu haline gelmiştir (Kara 2013).

3.1.1 Siber Ölüm Zinciri

Servis ve uygulamalardan oluşan ve klasik olarak adlandırılabilecek güvenlik zafiyetlerine karşı yama yönetimi yapılarak önlem alınabilir. Kolay parola kullanılması ya da ön tanımlı (default) parola kullanılması gibi daha çok kullanıcıların bilinçsiz olmasından kaynaklanabilen zafiyetlere de kullanıcıları bilinçlendirerek önemli ölçüde çözüm bulunabilir. Ancak gelişmiş siber saldırı olarak adlandırılan saldırılara bu kadar kolay önlem almak bir yana tespit etmek, saldırının derinliğini anlamak, etkisini tespit etmek bile çok zordur. Gelişmiş siber saldırı ele alındığında ortaya büyük, karmaşık ve sistemli bir saldırı hareketi çıkmaktadır. Bu yüzden de bu büyük resmi görmek içinde neler olduğunu anlamak mümkün olmamaktadır, mümkün olsa bile kolay olmayacaktır. Bundan dolayı güvenlik uzmanları bu gelişmiş siber saldırıyı belirli aşamalara ayırıp ele almışlardır.

Hutchins vd. (2011) siber ölüm zincirini; keşif (reconnaissance), silahlanma (weaponization), iletme (delivery), istismar/sömürme (exploitation), kurulum (installation), komuta ve kontrol (command and control – C'), amaca göre eylem (actions on objectives) olmak üzere yedi aşamaya ayırmışlar.

Keşif aşamasında saldırganlar hedef hakkında web sitesi, e-posta adresleri, çalışan bilgileri vb. bilgileri toplarlar ve hedef seçerler. **Silahlanma** aşamasına geçildiğinde ise zararlı yazılımı hedefe nasıl bulaştıracaklar ise o araçlar hazırlanır. Yani Word dokümanı mı iletilecek, pdf dokümanı mı iletilecek karar verilir ve bu dokümanlara

zararlı yazılım eklenir. **İletim** aşamasına geçildiğinde ise hazırlanan zararlı içerik veya siber silah hedefe gönderilir. Burada e-posta ile gönderme, kurum ile ilgili forum vb. sosyal ortam üzerinden gönderme, usb ya da CD gibi donanımlar ile gönderme gibi farklı yöntemler kullanılabilir. **İstismar/sömürme** olarak adlandırılan aşamada ise hedefe ulaşan siber silah, iletilen zararlı dokümanın açılması vb. sonucu aktif hale gelir. İstismar aşamasında ele geçirilen yetki ya da haklar üzerinde kalıcılığı sağlama veya hedefe kalıcı olarak yerleşme işlemi ve izleri silip kendini saklama **kurulum** aşamasında gerçekleşir. **Komuta ve kontrol** aşamalarında kendini gizlemiş olan zararlı yazılım şifreli kanallar üzerinden merkez sunucuyla haberleşmeye başlar. Artık bu aşamada saldırganlar iç ağda çalışan bir kullanıcı konumundadırlar. Yetki artırma vb. teknikleri uygularlarsa iç ağdaki birçok kullanıcıdan daha fazla yetkiye sahip şekilde faaliyetlerini yürütebilirler. APT saldırılarının son aşamasında ise esas **hedefe hizmet** edilir. Daha önce de bahsedildiği üzere bu ölçekteki büyük saldırılar "hedefli saldırılar" olarak da adlandırılır. Artık saldırının amacı ne ise o yönde bilgi çalma vb. özelleşmiş hedefler yerine getirilir.

Savunmacıların siber ölüm zincirinin herhangi bir aşamasında karşı atak yapma imkânı olmasına rağmen, kurumların üçüncü faz olan "iletim" gerçekleşmeden saldırı girişimine müdahale etmeleri mümkün olmamaktadır. Bunun nedeni ilk faz olan bilgi toplama açık kaynaklar üzerinden de yapılabileceğinden dolayı hedefin bunu tespit edip müdahale etmesi teknik olarak kolay olmamaktadır (Lachow 2013). Günümüzde internet ortamında insanlar kendileri hakkında çok fazla şey paylaşmaktadırlar. Ayrıca kurumların yaptıkları işler, ihaleler, işe alımlar vb. dokümanları iyi niyetle hatta belki bazen şeffaflık amacıyla internet vasıtasıyla kamuoyuna açtıkları aşikârdır. Ancak bundan faydalanmak isteyen bilgisayar korsanları çeşitli arama motorlarını kullanarak çok kolay bir şekilde kurumlar ve kişiler hakkında bilgi toplayabilmektedir. Hedef kurum hakkında bu şekilde bilgi toplayan saldırganı yakalamak çok kolay olmayacaktır.

3.1.2 Yaşanmış APT Saldırılarından Örnekler

Aktif siber savunmanın neden gerekli ve önemli olduğunu daha iyi anlamak için gelişmiş siber saldırıları incelemek faydalı olacaktır. Gelişmiş siber saldırılarda saldırganlar sistemlerde ne kadar süre kalıyor, ne kadar miktarda veri kaçırıyor vb.

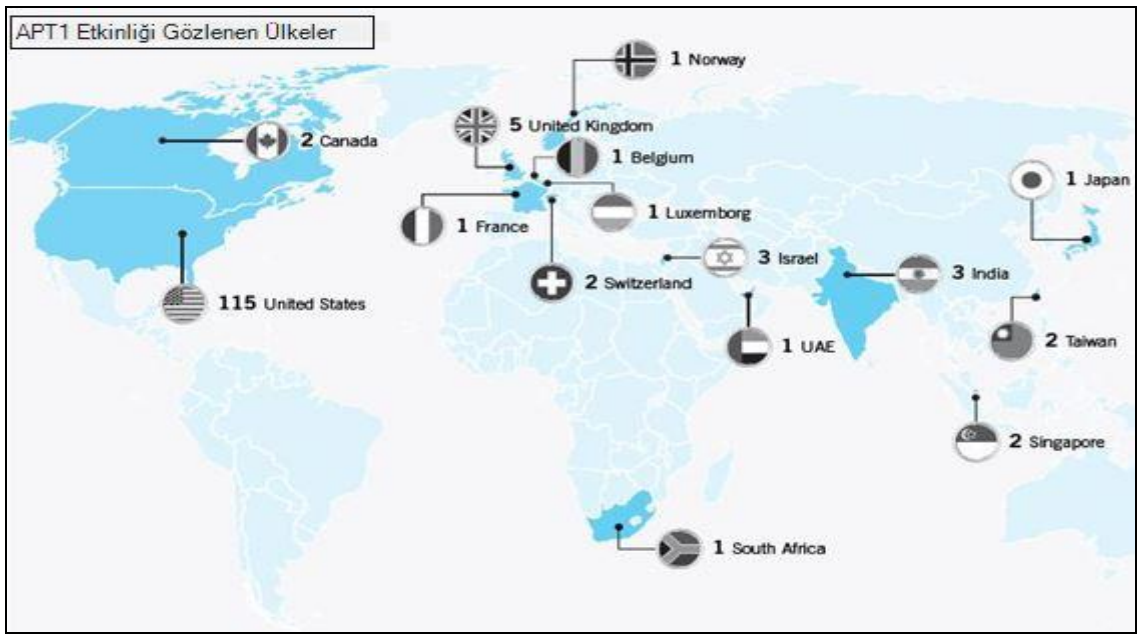
verilere bakıldığında aktif siber savunma yöntemlerinin önemi daha iyi anlaşılacaktır.

3.1.2.1 APT1

Mandiant (İnt.Kyn.4) tarafından Şubat 2013'te yayınlanan APT1 raporu gelişmiş siber saldırıların vahametini anlama açısından oldukça önemlidir. Çin Halk Cumhuriyeti'nin casusluk (espiyonaj) faaliyetleri yürüten yirmiden fazla olan APT gruplarından biri olduğunu ifade eden Mandiant bu grubu APT1 olarak adlandırmış ve bu raporda bu grup ve faaliyetleri hakkında detaylar paylaşmış.

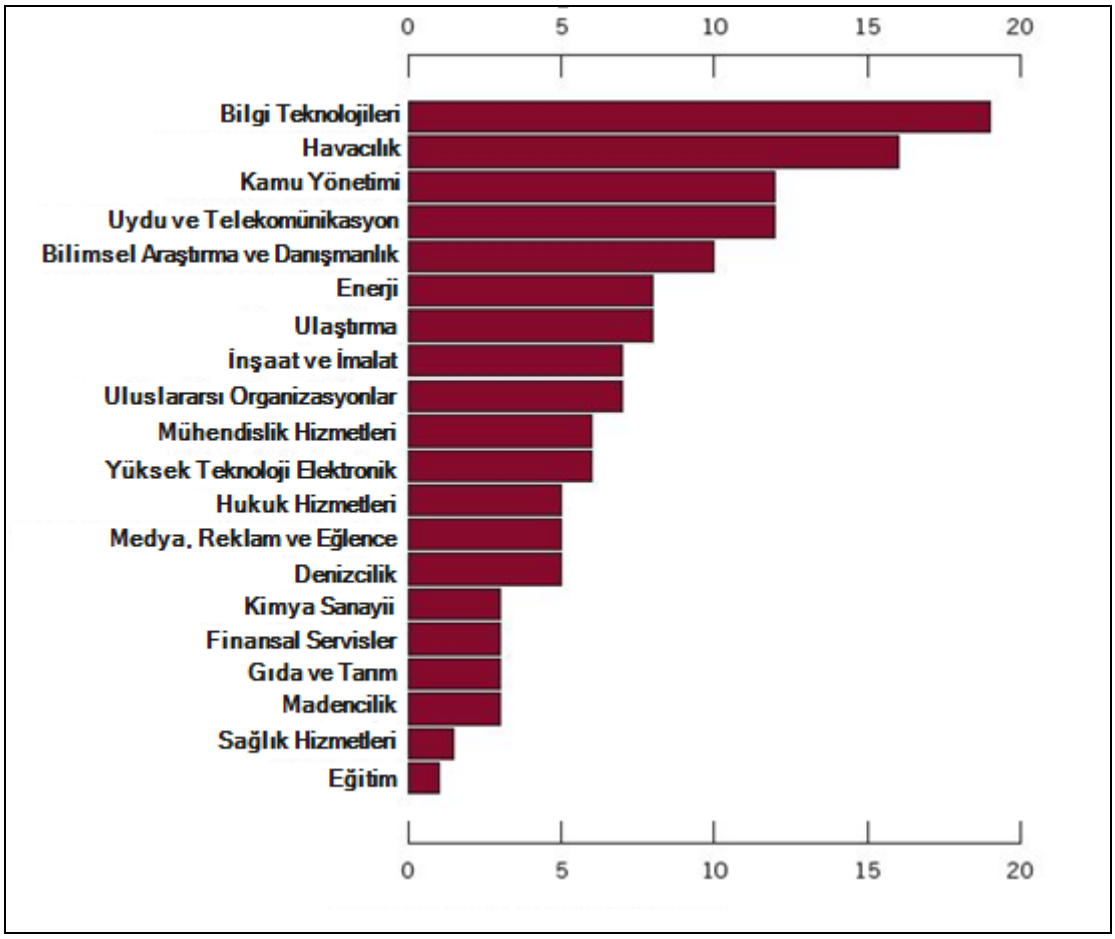
Raporda belirtildiği üzere Mandiant 2006-2013 yılları arasında APT1 grubunun 20 ana sektörde 141 firmaya sızdığını ve yüzlerce terabayt veri çaldığını tespit etmiştir. Bu grubun sızdığı kurbanlarının ağında ortalama 356 gün kaldığı belirtilmiştir. Ayrıca en uzun süre kaldığı kurbanın ağında ise 4 yıl 10 ay süre ile kaldığı tespit edilmiştir.

APT1'nın saldırısına uğrayan ülkeler ve o ülkeden kaç kuruma sızdığını gösteren harita Şekil 3.1'de görülmektedir. Şekilden de anlaşılacağı üzere ve raporda da belirtildiği gibi APT1'nın hedefinde ana dili İngilizce olan ya da İngilizce aktif olarak kullanılan ülkeler olduğu görülmektedir.



Şekil 3.1 APT1'nın sızdığı ülkeler (İnt.Kyn.4).

Gelişmiş siber saldırıların devlet destekli ve hedefli saldırılar olduğu anlatılmıştı. Mandiant'ın raporda paylaştığı grafikte kurbanların sektörlere göre sınıflandırmasına bakıldığında bu durum daha da iyi anlaşılacaktır. Şekil 3.2'de hedefteki sektörler ve hangi sektörde kaç organizasyona sızdığı gösterilmiştir.

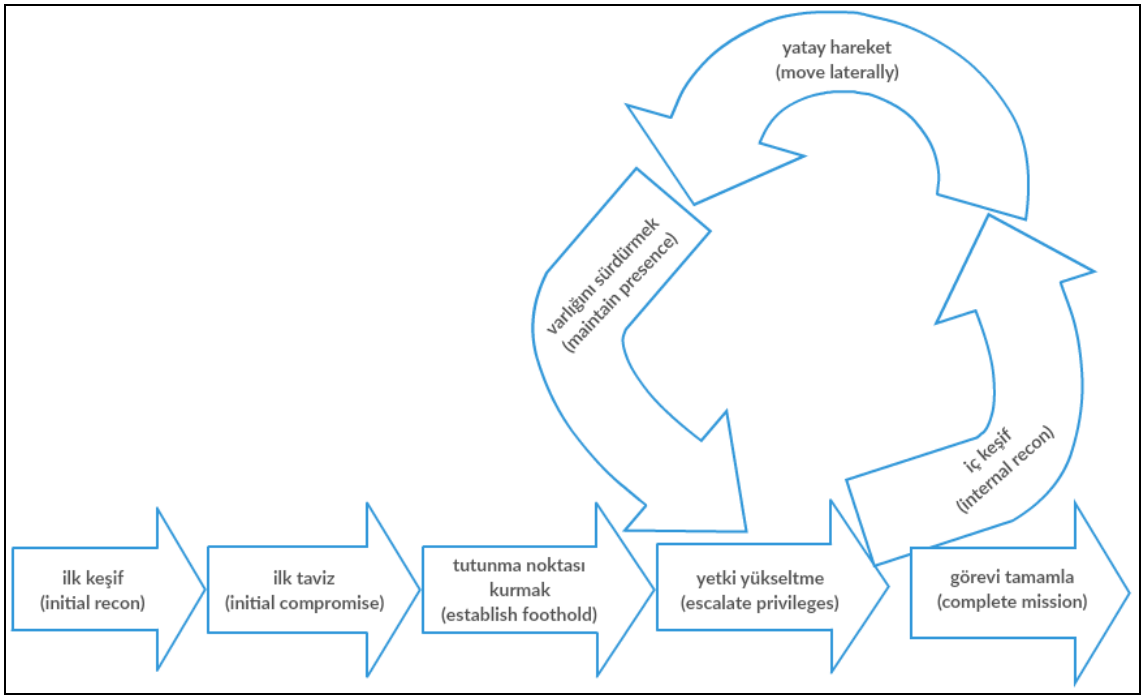


Şekil 3.2 Sektörlere göre APT1'nın sızdığı firma sayısı (İnt.Kyn.4).

Raporda APT1'in sızdığı kurbanlarından çok fazla veri çalındığı belirtilmektedir. Ne tür veriler çalınmış diye detaya inildiğinde ürün geliştirme, sistem tasarımı, test sonuçları, üretim süreçleri, standartlar, iş planları, politik analiz dokümanları, üst düzey kişilerin e-postaları ve kullanıcı bilgileri gibi birçok türde veri çalındığı görülmektedir. Bu bilgilerin birçoğu sıradan bir saldırganın eline geçse çok fazla bir şey ifade etmeyecektir ya da bunu parasal değere çevirmesi çok kolay olmayacaktır. Bundan dolayı da gelişmiş siber saldırılan devlet destekli olduğu düşünülebilir. Sadece tek bir firmadan 10 aydan fazla sürede 6,5 terabayt veri çalındığı belirtilmiştir. Bundan dolayı da saldırılar

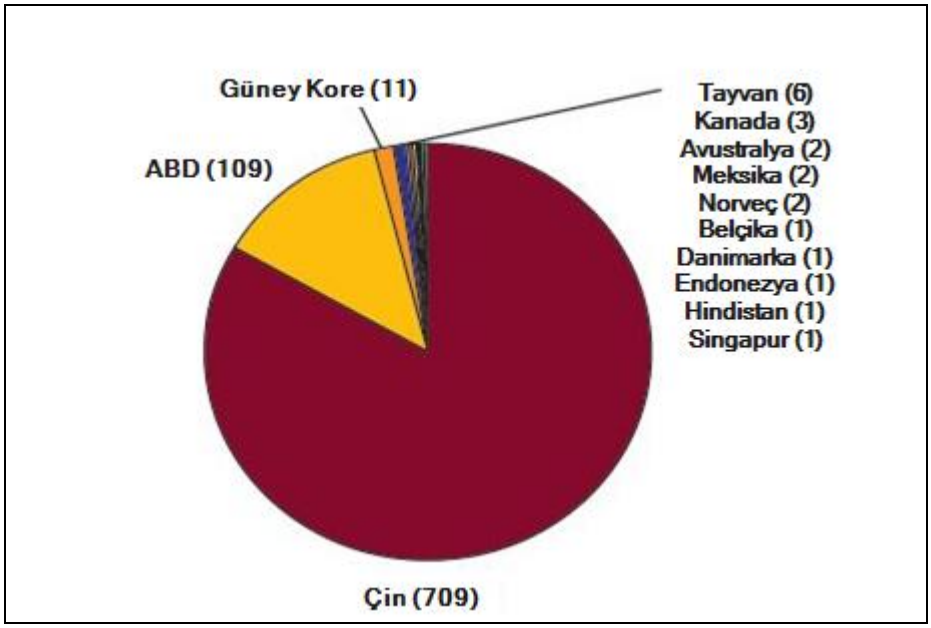
toplamında yüksek miktarda veri çalındığı tahmin edilmektedir.

Mandiant, APT1'nın saldırı analizini detaylı olarak bu raporda paylaşmıştır. Gelişmiş siber saldırıları daha iyi anlamak ve daha kolay analiz etmek için kullanılan siber ölüm zinciri yaklaşımına benzer şekilde Mandiant "Saldırı Yaşam Zinciri Modeli" olarak saldırıyı aşamalara ayırmıştır. Şekil 3.3'te bu model görülmektedir.



Şekil 3.3 Mandiant'ın saldırı yaşam zinciri modeli (İnt.Kyn.4).

Mandiant'ın raporda belirttiği bir diğer nokta ise APT1'nın kurbanlara doğrudan bağlanmak yerine vekil sunucular (Proxy server) kullandığı ve bu sunucuların farklı yerleşkelerde olduğudur. Gelişmiş siber saldırıların tespit edilmesi ve pasif sistemlerle engellenmesindeki zorluklardan bir tanesi de saldırının farklı ülkeler üzerinden yapılıyor olmasıdır. Raporda, APT1 grubunun sunucuları ve hangi ülke üzerinde kaç tane olduğu belirtilmiştir.



Şekil 3.4 Doğrulanmış APT1 sunucularının ülkelere göre dağılımı (İnt.Kyn.4).

Şekil 3.4'ten de anlaşılacağı üzere pasif savunma sistemlerinden olan güvenlik duvarına kural girerek düşman olan bir ülke için gelen ve giden tüm trafik engellemiş olsa dahi o ülkeden gelecek saldırılar engellemiş olmayacaktır. Sadece ilgili ülkeden doğrudan gelen trafik engellemiş olacaktır.

3.1.2.2 APT30

FireEye (İnt.Kyn.3) tarafından yayınlanan raporda yoğun olarak Güneydoğu Asya ve Hindistan'ı hedef aldığı belirtilen grup APT30 olarak adlandırılmıştır. Yapılan araştırmalarda bu grubun on yıl gibi bir zaman diliminde bölgedeki devlet ve ticari kuruluşların ağına sızdığı tespit edilmiştir.

Raporda dikkat çeken önemli bir nokta ise grubun internetten erişim olmayan intranet olarak adlandırılan ağlara sızdığı buralardan bilgi çalmaya çalışmış olmasıdır. Raporda belirtildiği üzere grubun aktivitelerine ve kullandığı araçlara bakıldığında hedefinde politik, askeri ve finansal verileri çalmak olduğu gözlemlenmiştir.

Bu raporun da desteklediği gibi gelişmiş siber saldırılar bilinen saldırıların aksine daha karmaşık ve zor saldırılardır. Ayrıca bilgisayar korsanları zamana karşı yarışmaktan

ziyade ağda dikkat çekip yakalanmamak için saldırıları geniş zaman diliminde yaparlar. Gelişmiş siber saldırıların hedefinde küçük ekonomik kazanç ya da ses duyurma gibi hedeflerden çok şahıslardan ziyade devletler için önem arz eden yüksek miktarda veri çalmak vardır. Bu nedenle karmaşık yapıda olan bu saldırılar karşısında pasif savunma sistemleri yetersiz kalmaktadır.

3.1.2.3 Shady RAT

Güvenlik şirketi olan McAfee 2011 yılında "Shady RAT" olarak adlandırılan büyük bir sızma (hacking) olayını ortaya çıkarttı. Bu saldırıyı yapan grubun, 14 ülkede elektronik, taşıma, savunma, haberleşme vb. alanında faaliyet gösteren ve özel ve devlet kurumları ile gönüllü kuruluşlar olmak üzere toplamda 71 kurumun ağına sızdığı tespit edilmiştir. Bu saldırı ile sızdırılan verinin bir petabyte (1000 terabyte) civarında olduğu tahmin edilmektedir (Alperovitch 2011).

3.2 Aktif Siber Savunma (Active Cyber Defense - ACD)

Mitnick, vd. (2003)'nin de belirttiği gibi alınan birçok önleme geliştirilen birçok yeni donanım ve yazılım çözümüne rağmen bilgi sistemlerine yönelik güvenlik saldırıları her geçen gün hızla artmaktadır. Bilginin gizliliğine, bütünlüğüne, erişilebilirliğine karşı yapılan saldırılar ciddi ve giderilemeyecek kayıplara yol açmaktadır. Bu kayıpları tamamen yok etmek mümkün değildir. Ancak önceden veya zamanında alınacak güvenlik tedbirleriyle kayıpları en aza indirmek mümkündür (Vural *et al.* 2009).

Gelişmiş siber saldırılar karşısında geleneksel güvenlik sistemlerinin yetersiz kalmasından sonra geliştirilen aldatma, yavaşlatma ve karşı atak gibi daha dinamik çözümler veya yaklaşımlar aktif siber savunma teknikleri veya aktif siber savunma yaklaşımı olarak literatüre girmiştir.

Amerika Birleşik Devletleri (ABD) ordusu aktif savunmayı, sınırlı ölçüde saldırgan eylemler ve karşı saldırılar yaparak düşmanın avantajlı duruma geçmesini engellemek olarak tanımlamaktadır (McGee *et al.* 2013). Aktif siber savunma, siber saldırı

öncesinde ve sırasında saldırganı engellemeye yönelik proaktif eylemler dizisidir. Aktif siber savunma, karmaşık siber saldırıları tespit etme, önleme ve cevap verme çabalarını artırmaktadır (Lachow 2013). Diğer bir yaklaşımla da aktif siber savunma, tehdit ajanları etkisizleştirmek için tasarlanmış saldırgan dış tekniklerin yanı sıra, kötü niyetli kodlara ve diğer saldırılara karşı proaktif önlemler içeren siber güvenlik yaklaşımıdır (Lu *et al.* 2013).

Güvenlik duvarı ve saldırı önleme sistemi/saldırı tespit sistemi (intrusion prevention system/intrusion detection system – IPS/IDS) gibi güvenlik çözümleri gelişmiş siber saldırılara karşı koyamadığı için aktif siber savunma teknikleriyle saldırılar engellenmeye veya yavaşlatılmaya çalışılmaktadır. Ayrıca karşı ataklar yaparak saldırganları durdurmaya çalışmak da aktif siber savunma konsepti içinde yer almaktadır.

Tüm tehditlerin önlenemeyeceği kabul edildiğinde, geleneksel güvenlik önlemleri ile zararlı yazılım tespit edilmemiş olsa bile şu anda risk altında olan sistemlerde; olayları tespit etme ve cevap verme hızı kritiktir (Pingree *et al.* 2013). Pasif savunma saldırganların kazanç olasılığını azaltmaktadır ancak pasif savunmanın yeteneği savunucuyu korumak için sınırlıdır (Anderson *et al.* 2005).

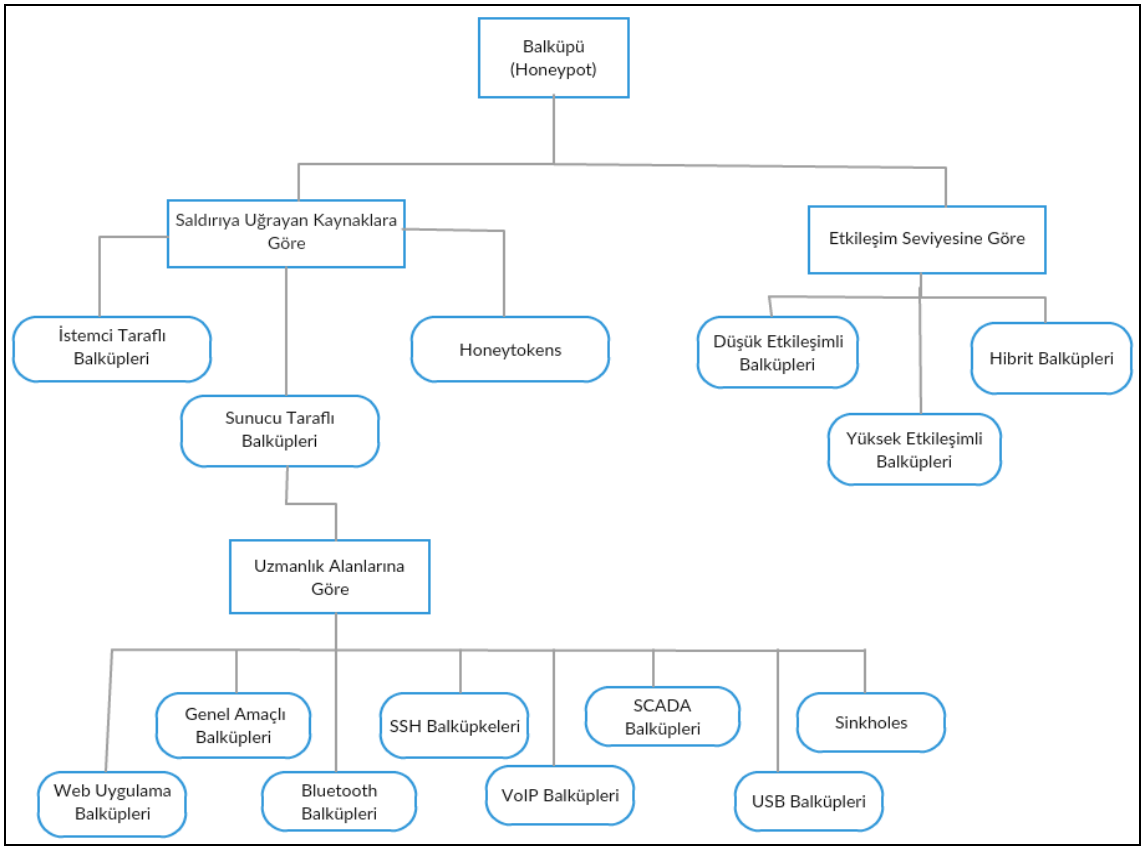
Gelişmiş siber saldırıların yapılmasındaki önemli faktörlerden biri de saldırgan tarafın kurbanlara ait askeri, politik ve ticari öneme sahip gizli ve kritik bilgileri çalmak olduğu için saldırganın yanlış bilgilere ulaşmasını sağlamak da aktif siber savunma yaklaşımı içine girmektedir. Bundan dolayı saldırgan hakkında bilgi toplamak ne tarz bilgilere erişmeye çalıştıklarını bilmek önem arz etmektedir.

Gelişmiş siber saldırılar karmaşık yapıda olduğu için bu saldırılarla mücadele etmek ve karşı koymak zor olmaktadır. Aldatma, yavaşlatma ve karşı atak gibi savunma yaklaşımlarını kullanmak için siber saldırıyı iyi analiz etmek gerekmektedir. Bundan dolayı Hutchins vd. (2011)'nin yaptığı gibi gelişmiş siber saldırıları parçalara ayırıp doğru aşamada doğru savunma yaklaşımı kullanılarak saldırılara karşı çözüm üretilebilir.

3.2.1 Balküpü (Honeypot)

Saldırganları tespit etmek, yaptıkları saldırıları analiz etmek ve/veya saldırganları yavaşlatmak, yanlış bilgileri ele geçirmelerini sağlamak gibi kurulum amacına göre yapısında da farklılık gösteren ağ sistemlerine balküpü (honeypot) denilmektedir. Bir başka balküpü tanımı ise şöyledir; bilişim sistemlerine karşı gerçekleşen saldırıların tespit edilmesi için kurulmuş olan tuzaklardır (Soysal *et al.* 2015).

Balküpü, tuzak sistemlerinden oluşan bir ağdır. Açık kaynak kodlu yazılımlarla bu tür sistemler kurmak ve yenilerini geliştirmek mümkündür (Karaarslan *et al.* 2008). Balküpleri kuruluş amaçlarına, saldırgan ile etkileşimlerine vb. özelliklerine göre sınıflandırılırlar. ENISA (European Union Agency for Network and Information Security) tarafından yapılan sınıflandırmanın grafiksel gösterimi Şekil 3.5'te gösterilmiştir.



Şekil 3.5 Balküplerinin sınıflandırılması (Grudziecki *et al.* 2012).

Üzerlerinde saldırganların dikkati çekecek hizmetler sunarlar (ssh, telnet vb.) (Soysal *et al.* 2015). ENISA tarafından yapılan bu çalışma incelendiğinde sunucu taraflı balküplerinin sunucularda çalışan servisleri (ssh, telnet, voip, web uygulaması) taklit ettiği ve bu servislere yönelik yapılan saldırıları tespit etmeye yönelik yapılan çalışmalarda kullanıldığı görülmektedir.

Kullanıcı taraflı balküpleri olarak adlandırılan uygulamalar ise sunucu tarafından farklı olarak kullanıcı hareketlerini taklit ederler. Kullanıcı tarafında en çok hedef olan uygulamalar tarayıcılarla birlikte eklentiler ve uzantılardır. Kullanıcı uygulamalarına yönelik saldırıları tespit etmeyi amaçlayan bu balküpleri sunucularla etkileşim kurarak web aracılığıyla yayılan zararlı yazılımları tespit etmeye yönelik çalışırlar (Grudziecki *et al.* 2012).

Balküpleri, etkileşim seviyesine göre düşük ve yüksek etkileşimli olmak üzere ikiye ayrılabilir. Düşük etkileşimli balküpleri sunucu taraflı ya da kullanıcı taraflı ilgili servisi taklit eder. Saldırgan ile etkileşimleri gerçek servislere göre daha düşüktür. Düşük etkileşimli balküplerinin kurulması ve yönetimi kolaydır. Ancak sömürme (exploitation) araştırma süreçleri için uygun değildirler. Düşük etkileşimli balküpleri saldırganlar tarafından kolayca tespit edilebilmektedir (Grudziecki *et al.* 2012).

Yüksek etkileşimli balküpleri gerçek sistem ve kaynak sunan araçlardır. Yani bu sistemlerde taklitten ziyade gerçek sistemler kullanılmaktadır. Ancak sanal sistemler sayesinde bir nevi taklit etmek de mümkündür ve genel uygulamalarda sanal sistemler kullanılmaktadır. Bu konseptte saldırganın sanal sistemlerde etkileşimi sınırsızdır. Bundan dolayı sızma ve enjeksiyon süreçleri tamamen analiz edilebilir. Yüksek etkileşimli balküplerinin gerçek davranış sergilemesi temel avantajlarıdır. Sıfırıncı gün açıklığı gibi açıklıkları bu sistemler ile tespit etmek mümkündür (Grudziecki *et al.* 2012).

Etkileşim seviyesinin artmasıyla balküpünün ele geçirilmesi riski artmaktadır öte yandan saldırganların gerçek sistemle etkileşime girmeleri sonucu saldırgan ve saldırı hakkında daha fazla bilgi elde edilmektedir (Gökırmak *et al.* 2009).

Balküpü tasarımında dikkat edilmesi gereken bir nokta da balküpünün saldırganlar tarafından algılanmamasını sağlamaktır. Saldırgan, etkileşimde olduğu sistemi bir balküpü olarak değil gerçek bir servis olarak algılamalıdır (Gökırmak *et al*. 2009). Balküpü mümkün olduğunca genel gözükmelidir. Eğer Microsoft NT tabanlı sistem kullanılırsa, potansiyel saldırgan için sistem modifiye edilmemiş görünmeli, aksi takdirde saldırgan hakkında yeteri kadar bilgi toplanmadan saldırgan sistemden çıkabilir (Even 2000).

Balküpleri, ele geçirme amacıyla kurulmuş bilgisayar kaynaklarıdır. Balküpleri güvenlik duvarlarını ve saldırı tespit sistemlerini zararlı aktivitelerin tespiti karşısında güçlendirmek için kullanılır. Bazı balküpleri sadece bilgisayar korsanı tarafında aranan servisi sağlamaz buna ilaveten saldırganın ağı taraması karşısında işletim sisteminin parmak izini taklit eder. Bir saldırı durumunda savunma tarafındaki ağdaki gerçek makinelere yeni adres verip çalışan sistemleri balküpleri ile değiştirebilir ve böylece daha çok network var gibi gösterebilir (Dittrich and Himma 2005).

Balküpü ile geleneksel internet güvenlik sistemlerinin yer değiştirmeyeceği unutulmaması gereken önemli bir husustur. Onlar ilave bir katman ya da sistemdir. Balküpü, güvenlik duvarı tasarımında iç ağa, dış ağa ya da askerden arındırılmış bölge (demilitarized zone –DMZ) bölgesine kurulabilir veya onlar tüm ağ içinde olmalarına rağmen kontrol amacıyla daha sık olarak güvenlik duvarının içine yerleştirilir. Bir anlamda, onlar standart sızma tespit sistemlerinin (IDS) bir parçasıdır fakat daha çok bilgi toplama ve aldatmaya odaklanır (Even 2000). Saldırganların hedeflere karşı davranışlarını anlayarak, savunucular güçlü taktik, teknik ve prosedürler üretebilirler (İnt.Kyn.1).

Genel olarak bal küpü kullanmanın amacı:

- Saldırganların sistemlere erişmek için nasıl araştırma yaptığını ve teşebbüs ettiğini öğrenmek.
- Davetsiz misafirin yakalanması veya kovuşturmaya yardımcı olmak için gerekli adli bilgiler toplamak

olarak belirtilmiştir (Even 2000).

Balküpü kurumun izleyebileceği farklı tipte doküman ile kurulursa saldırgan bazı dokümanları seçer. Bu sayede saldırganın motivasyonu hakkında bilgi ve saldırganın belirlenmesi için ipuçları elde edilebilir. Özellikle kurum farklı aktörlerin operasyon ve stratejik istihbaratlarını elde etme imkânı bulduysa (Lachow 2013). Örneğin Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) gibi birden çok alanda faaliyet gösteren bir kuruma yapılan saldırıda, saldırganın hangi alanda yapılan çalışmaları bulmayı hedeflediğinin tespit edilmesidir.

Balküpleri zafiyet içeren uygulamalar ya da sunucular olduğu için ele geçirilme ihtimalleri de vardır. Özellikle yüksek etkileşimli balküpleri gerçeğe yakın sistemler olduğu için üzerinde çalışan birden fazla servis, uygulama vs. vardır. Bundan dolayı ele geçirildiğinde bu balküpü üzerinden diğer ağ ve sunuculara yönelik saldırı yapılmasını engellemek adına doğru yere kurulmalı ve güvenlik duvarı üzerinden diğer ağlara erişimi kısıtlanmalıdır.

3.2.2 Dünyada Aktif Siber Savunmaya Bakış ve Örnekler

Bilinen ilk siber saldırı örneklerinden Cuckoo's Egg (guguk kuşu yumurtası) saldırısı 1986 yılında Lawrence Berkeley Ulusal Laboratuvarına (LBUL) yönelik gerçekleştirildi. Güvenlik uzmanı Stoll, arkadaşının uyarısı sonrasında yaptığı çalışmada sistemlerinde bir saldırgan olduğunu fark etmiştir. Ancak saldırgana müdahale etmek yerine saldırganın ağdaki hareketlerini izlemeyi tercih eden Stoll, saldırgan hakkında yeterince bilgi elde etmiştir. Saldırganın ağda nükleer sistemler hakkında bilgi aradığını tespit eden Stoll LBUL sisteminde 'SDInet' adlı bir hesap açmıştır ve yeterince ikna edici bilgilerle doldurmuştur. Tuzak bir bilgiyi sisteme yerleştiren Stoll saldırganın ağda çevrimiçi kalmasını sağlayarak izini sürmüştür, saldırganı tespit etmiştir ve ülkesinde yakalanmasını sağlamıştır (İnt.Kyn.18). İlk balküpü sistemlerine de örnek olabilecek bir yaklaşım ile saldırganı aldatıp hakkında detaylı bilgi toplayarak yakalanmasını sağlamak aktif siber savunma yaklaşımına örnek teşkil etmektedir.

Gelişmiş siber saldırılarda hedefteki ülke ya da kurumun sahip olduğu ekonomi programları, teknoloji veya savunma sanayi alanında yaptığı yatırımlar, politik

çalışmalar vb. kritik bilgiler ele geçirilmeye çalışılmaktadır. APT1 gibi tespit edilen gelişmiş siber saldırılarda çalınan veriler de bu durumu doğrulamaktadır. Bu yüzden Lachow'un (2013) da belirttiği gibi aldatma sadece saldırı için değil savunmayı güçlendirmek için saldırgana karşı da kullanılabilmektedir. Saldırganın yanlış bilgileri ele geçirmesini sağlayarak aldatmanın da aktif siber savunma kapsamında kullanılabileceği belirtilmektedir.

Aktif siber savunma teknolojilerinin en son aşırı noktasında, saldırganı yok etmek ya da ekonomik zarar vermek için saldırganların sistemlerine karşı saldırı olarak dağıtık servis dışı bırakma (DDOS) saldırısı yapılabilir. Küçük ölçekli tarayıcı temelli servis dışı bırakma saldırıları (DOS), tarayıcıdaki açıklığı sömürmek için zararlı kod göndererek bertaraf edilebilir. Bu teknik Pentagon tarafından başarılı bir şekilde kullanıldı (Anderson *et al.* 2005).

İş modelini 'aktif siber savunma' olarak benimsemiş şirketler bulunmaktadır. Bu şirketler kuruma saldıran bilgisayar korsanlarını siber alanda bulup cezalandırmayı, onları bir daha kuruma saldırmayacak hale getirmeyi taahhüt etmektedirler. Onlara ek olarak, Sony gibi büyük firmalar kendi bünyelerinde 'aktif siber savunma' birimi kurmaktadırlar. 2015 yılında yaşanan Sony saldırısından sonra bilgisayar korsanlarına karşı saldırı yapılması bu durumun en anlamlı örneklerinden birini oluşturmaktadır (İnt.Kyn.15).

ABD Başkanı Obama'nın artan siber saldırılar ve son olarak da Sony'ye yönelik Kuzey Koreli saldırganlar tarafından yapılan siber saldırılar sonrasında yaptığı açıklamada seviyeli olarak bu saldırılara cevap vereceği belirtilmektedir (İnt.Kyn.18). Siber saldırılar karşısında yapılacağı belirtilen bu karşı ataklar da aktif siber savunma yaklaşımına örnektir.

Sony'nin DDOS kullanarak aldığı önlem, firmanın korsan dosyaların belirmeye başladığı ilk zamanlarda MediaDefender firmasıyla geliştirdiği yönteme benzetilmektedir MediaDefedner, Örümcek Adam gibi zamanın ünlü filmlerine ait sayısız sahte dosya üretilmekte ve korsan dosya indirmek isteyenler saatlerce boş bir

dosyayı indirerek vakit harcamaktadır (İnt.Kyn.13). Kamu kurumları da ağlarına kuracakları gerçeğe yakın balküpleri ile saldırganları yavaşlatabilirler.

Sanal hippiler, Conxion'nun sunucularına servis dışı bırakma saldırısı (DOS) yapmışlardır. Conxion gelen saldırı paketlerini saldırganların ağına geri yönlendirdi. Bu karşı atak saldırıyı durdurmada başarılı oldu. Ancak bu durum aynı zamanda biraz cezalandırıcı olmuştur çünkü Conxion paketleri yönlendiricide düşürerek basitçe bu saldırıyı bitirebilirdi (Dittrich and Himma 2005).

Çin Halk Cumhuriyeti Savunma Bakanlığı (2015) yayınladığı askeri strateji taslağında siber güvenliğe önem verdiğini ortaya koymaktadır. Strateji dokümanında dikkat çeken önemli bir özellik, hücuma dayalı (ofansif) siber kabiliyet geliştirme konusu 'siber savunma' kapsamı içerisinde meşrulaştırılıyor olmasıdır. Strateji belgesinde geçen 'Saldırıya uğramadan saldırmayacağız fakat saldırıya uğrarsak muhakkak karşı saldırıda bulunacağız." kesin ifadeleri silahlı kuvvetler bünyesinde ofansif siber kabiliyetler bulunduğunun da bir göstergesi olarak kabul edilebilir. Diğer bir ifadeyle stratejik seviyedeki 'savunma' konseptinin operasyonel ve taktik seviyelerde ofansif adımlar atmayı gerekli kılabilecek şekilde esnetebileceği belirtilmektedir (İnt.Kyn.14).

3.2.3 Aktif Siber Savunma Tekniklerinin Uygulamasında Hukuki Kısıtlamalar

Aktif siber savunma konsepti içinde karşı atak teknikleri de bulunduğu için savunucular saldırı yapmak durumundadırlar. Bu durum hukuki çerçevede önem arz etmektedir. Bu çalışmanın amacı ve kapsamı işin hukuki yönünden bağımsız olarak sadece aktif siber savunmanın teknik boyutları üzerinde çalışmaktır. Buna ilaveten aktif siber savunmanın hukuki yönden ne gibi sorunlar oluşturabileceği de kısaca anlatılacaktır.

Gelişmiş siber saldırıların tecrübeli bilgisayar korsanları tarafından yapıldığından ve devlet destekli büyük saldırılar olduğundan bahsedilmişti. Bundan dolayı böyle bir saldırı ortaya çıktığında uluslararası hukukun devreye girmesi gerekecektir. Ancak siber saldırıların kaynağını farklı göstermek çok daha kolaydır. Bir ülkeye bir füze ya da roket gönderildiğinde bunun hangi ülke tarafından gönderildiğini, füzenin özellikleri, menzili ve kullanılan teknoloji sayesinde hangi ülkeden geldiğini tespit etmek daha

kolay olabilmektedir. Bir başka açıdan ele alındığında ise bir ülkeye füze göndermek vb. girişimler bir savaş sebebi olabileceği için ve dünya kamuoyu tarafından da tepki gösterileceği için böyle bir aksiyon almak kolay değildir veya ciddi bir gerekçe gerektirmektedir. Ancak siber saldırılarda durum daha farklıdır. Her ülkede farklı ülkelerin istihbarat ajanların vardır ve istihbarat kurumları imkânları dâhilinde ve karşılıklı ilişkilere göre o ülke hakkında ekonomik, politik vb. konular hakkında bilgi toplamaya çalışır (İnt.Kyn.14). Ancak bu ajanlar pasif dinlemeden aktif çalışmaya ya da bir operasyona giriştiklerinde yani istihbarat ajanı olduğuna dair somut delil elde edildiğinde sınır dışı edilirler ya da hukuki süreç başlar.

Gelişmiş siber saldırı örneklerine bakıldığı zaman ortaya çıkan tablo bir nevi istihbarat çalışmalarıyla benzerdir. Saldırıyı gerçekleştirenler, hedeflerinin ekonomik, teknolojik, politik vb. alanlardaki yaklaşımları, geliştirdikleri teknolojileri öğrenmeye ve çalmaya çalışırlar. Fakat gelişmiş siber saldırıların adresinin tam olarak belli olmaması hukuki süreçleri daha da zor durumda bırakmaktadır. Çünkü saldırının geldiği adres gerçek saldırıyı yapan yer olmayabilir, aksine o da siber saldırı kurbanı olup bir başka saldırı için tünel olarak kullanılıyor olabilir. Bundan dolayı buraya yönelik yapılacak bir saldırı ayrı bir hukuki sorun doğurabilir.

Bilişim suçlarının ve siber güvenlikle ilgili eylemler hukukta tam olarak karşılığını bulamamıştır. Önemli tartışma konularından bir tanesi bu faaliyetlerin hangi devlet sınırları içerisinde yapıldığı ile alakalıdır. En nihayetinde bu eylemler belirli devlet politikaları açısından suç oluşturabileceği gibi, devletlerin belirli amaçlarına hizmet ettiği de düşünülebilir (İnt.Kyn.10).

Bir siber saldırıya karşı atak ile cevap verilmek istendiğinde ne kadar şiddetli saldırı ile cevap verilecek olması bir başka hukuk sorusudur. Ayrıca aktif siber savunma yaklaşımı çerçevesinde gündeme gelen bir başka nokta olan, saldırgan saldırmadan saldırı yapmak yaklaşımı da farklı bir hukuki konudur.

Bilişim suçları ile ilgili düzenlemeler ülkemizde son zamanlarda hazırlanmış ve kısıtlı sayıdadır. Bu alanda yapılan düzenlemeler 5237 sayılı Türk Ceza Kanunu'nun 3. kısım

10. bölümü ile 5651 sayılı İnternet Ortamından Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'dan oluşmaktadır (İnt.Kyn.10). Ülkemizde henüz aktif siber savunma alanında yapılmış hukuki bir düzenleme yoktur. Dünya hukuku ya da uluslararası hukuka bakıldığında durum yine benzerdir. Ancak ABD gibi gelişmiş siber saldırılardan zarar gören bazı ülkelerin karşı atak yapacakları konusunda yaptığı açıklamalar vardır (İnt.Kyn.12).

ABD Başkanı Barack Obama, son yıllarda artan siber saldırılara karşı Washington'un gerekli yaptırımları uygulamasına dönük bir karara imza attı. Bu imzanın ardından Washington'ın dış politikasını, ulusal güvenliğini ve ekonomik istikrarını hedef alan siber saldırganlara karşı yaptırım uygulanabilecektir (İnt.Kyn.15).

Aktif siber savunma yöntemlerine yönelik ülke içinde ve uluslararası düzenlemelere ihtiyaç vardır. Lachow (2013)'un da belirttiği gibi devletler hukuki düzenleme yapmazsa ve neyin yasal neyin yasa dışı olacağını açık bir şekilde ortaya koymazsa iki sonuç ortaya çıkabilir. Birincisi, kurumlar yasa dışı bir müdahale yaparız korkusu ile yasal olan bir önleme yöntemini bile kullanmayabilirler. İkincisi ise kurumlar yasal olduğunu düşünüp yasa dışı bir müdahaleyi çözüm olarak kullanabilirler.

3.3 Kamu Kurumlarında Siber Savunma ve Eksiklikler

Siber ortamda sayıları her geçen gün artan tehditleri bertaraf etmek ve ulusal siber ortamda bulunan açıklıkları mümkün olduğunca azaltmak, ülke olarak hedeflemekte olduğumuz bilgi toplumuna dönüşüm sürecinin sağlıklı bir şekilde ilerlemesi açısından büyük önem arz etmektedir. Bilgi toplumuna dönüşüm sürecinde, bilgi ve iletişim teknolojilerinin daha büyük kitleler tarafından etkin, kaliteli ve uygun maliyetle kullanılmasının yanı sıra, söz konusu teknolojilere dayalı bilişim sistemlerinin kullanımında siber güvenliğin tesis edilmesi de son derece önemlidir (Resmi Gazete 2013).

Geleneksel savunma sistemleri denildiğinde güvenlik duvarı, saldırı tespit ve önleme cihazı içerik filtreleme ürünleri gibi ağ cihazları ile yapılan savunma yaklaşımı akla gelmektedir. Ayrıca sunucuların, ağ cihazlarının ve uygulamaların güvenlik yamalarının

düzenli olarak yapılması da geleneksel savunma yaklaşımı konsepti içinde yer almaktadır.

Kamu kurumlarında siber güvenliği sağlamak adına geleneksel savunma sistemleri kapsamında bahsedilen ürünler kullandığı ve ağdaki sunucuları ve diğer ağ cihazlarının güncellemelerini yaptığı ve belirli güvenlik önlemlerini aldığı kabul edilebilir. Ancak zayıf halkanın insan faktörü olduğu yerlerde güvenlik açıklıkları olacaktır. Bu açıklıklar iki şekilde ortaya çıkar. Birincisi doğrudan kişileri hedef alan ve kişilerin bilinçsiz olması ya da zayıf noktalarının hedef alınmasından kaynaklı olup sosyal mühendislik saldırıları ile sömürülür. Diğeri ise savunma sistemlerinin güvenlik zafiyetine neden olabilecek şekilde eksik ya da yanlış yapılandırılmasından kaynaklı olup farklı teknik ve yöntemlerle sömürülür.

Siber tehditleri önlemenin veya en azından etkisini azaltmanın en etkin yollarından biri eğitimdir. Gerek bireysel olarak kendimizi gerekse kurumsal olarak personeli siber güvenlik konusunda eğitmek ve son bilgilerle donatmak artık kaçınılmaz hale gelmiştir. Bununla paralel olarak kurumlardaki ve bireysel kullanımdaki bilgisayarlar en son teknoloji ve güvenlik yazılımları ile donatılmalıdır (Öğün and Kaya 2013)

Sağlık sektöründeki güvenlik önlemlerinin yeterince iyi olmadığı bilinmektedir. 2014'ün son günlerinde yapılan bir araştırmada, bir devlet hastanesinde bulunan zafiyetler zinciri nedeniyle 600 000'den fazla hastaya ilişkin kritik kimlik bilgileri, iletişim bilgileri ve hastalığın ifşa edilebildiği görülmüştür. Bu zafiyet Sağlık Bakanlığı'nın ilgili birimleriyle paylaşılarak giderilmesi sağlanmıştır (Altundal 2014).

Güvenlik firması Symantec yayınladığı raporda 2014 yılında endüstriyel kontrol sistemlerine yönelik daha fazla saldırı gördüklerini belirtmektedir. Bu saldırılarda enerji operatörleri, elektrik jeneratörleri, petrol boru hattı operatörleri gibi kritik sistemler ve endüstriyel donanım üreticileri gibi kurumlar hedef alınmıştır. Bu saldırıların hedefinde olan büyük kurbanlardan bir tanesinin de Türkiye olduğu belirtilmiş (İnt.Kyn.5).

Her geçen gün artan siber saldırılar karşısında ülkemizdeki kişi ve kurumların da bu

saldırılardan nasibini aldığı güvenlik raporlarında ortaya çıkmaktadır. Bu raporlardan ülkemizdeki siber savunmanın yetersiz olduğu ve kişilerinde siber saldırılar karşısında yeteri kadar bilinçli olmadığı çıkarımı yapılabilir (Altundal 2014, İnt.Kyn.2).

Küresel olan siber tehditlerle yerel yaklaşımlar yoluyla mücadele etmek zordur; bu nedenle konuya ulusal yaklaşımlar getirilmeli ve ilgili uluslararası kuruluşlar ile olan işbirliği güçlendirilmelidir (Öğün and Kaya 2013).

4. METOT

Geleneksel savunma sistemlerinin gelişmiş siber saldırılar karşısında yetersiz olduğu anlaşılınca yeni çözümler aranmıştır. Aktif siber savunma yaklaşımları ve/veya teknikleri gelişmiş siber saldırılara karşı koyma çabası olarak ortaya çıkmıştır. Güvenlik duvarı, IPS/IDS gibi tekil sistemler ile bu saldırılara karşı koymak mümkün olmamıştır. Bundan dolayı daha dinamik çözümlerin arayışı içine girilmiştir.

4.1 Aktif Siber Savunma Teknikleri

Aktif siber savunma yaklaşımı ele alındığında **engelleme, yavaşlatma, karşı saldırı** ve **aldatma** olarak dört başlık altında toplanabilir. Gelişmiş siber saldırıları durdurmak her zaman mümkün olmadığı için kayıp ve zarar en aza indirilmeye çalışılmıştır. Bu çalışmaların sonucu olarak da aktif siber savunma yaklaşımları ortaya çıkmıştır.

Gelişmiş siber saldırılara karşı önceden belirli önlemler alıp saldırıyı kesin bir şekilde önlemek gibi bir durum söz konusu değildir. Yani güvenlik duvarına Secure Shell (ssh) servisine yönelik engelleme kuralı girildiğinde güvenlik duvarından ssh servisine yönelik hiçbir trafik geçmeyeceği iddia edilebilir ancak gelişmiş siber saldırılara karşı böyle bir kesinlik söz konusu değildir. Bundan dolayı aktif siber savunma Lachow (2013)'un da belirttiği gibi siber saldırı öncesinde ve sırasında saldırganı engellemeye yönelik proaktif eylemlerdir.
Gelişmiş siber saldırıları daha iyi analiz etmek ve etkili bir önlem alabilmek için siber ölüm zinciri modelinin kullanıldığı daha önce belirtilmişti. Siber ölüm zincirinin ilk adımı olan keşif aşamasında saldırganın işini zorlaştırmak ve keşif yapmasını yavaşlatmak adına farklı çözümler sunulmuştur. Ayrıca saldırı esnasında karşı saldırı yapmak gibi alınabilecek önlemler ile de saldırıları yavaşlatma amaçlanmıştır.

Aktif siber savunma yaklaşımı kapsamında değerlendirilen bir diğer çözüm ise karşı ataktır. Gelişmiş siber saldırılara tam anlamıyla karşı koyulamadığı için çözüm olarak düşman saldırmadan önce, düşmana saldırı yapıp yok etmek ve sistemlerine zarar vermek de önerilen aktif siber savunma konsepti içinde yer almaktadır.

Saldırıların meydana geldiği anda tespit edilmesi, bunlara karşı yeterli önlem ve müdahale imkânlarının bulunması kadar önemli bir faktördür. Elde gerekli yöntem, araç ve kabiliyetler bulunsa da iş işten geçtikten sonra yapılan bir müdahale anlam taşımayacaktır (Öğün and Kaya 2013). Aktif siber savunma yaklaşımları ile önceden tespiti mümkün olmayan veya saldırı esnasında dahi tespiti zor olan gelişmiş siber saldırılara karşı çözüm üretilmeye çalışılır.

4.2 Aktif Siber Savunmanın Siber Ölüm Zincirinde Yeri ve Etkileri

Siber ölüm zincirinin ilk aşaması olan keşif aşaması pasif ve aktif keşif olmak üzere ikiye ayrılır. Pasif keşif çalışmalarında saldırgan kurban hakkında internette açık olarak bulunan bilgileri toplar. Bundan dolayı kurbanların bu aşamada yapabileceği çok bir şey yoktur. Ancak aktif keşif aşamasına geçildiğince saldırganlar hedeflerindeki ağlar ile etkileşime geçip açık portları ve sistemlerdeki zafiyetler gibi daha teknik bilgiler toplamaya başlarlar. Nmap, nessus, zmap, scapy ve hping3 gibi keşif ve zafiyet tarama araçlarının kullanıldığı bu aşamada saldırıyı tespit etmek mümkün olabilir. Fakat gelişmiş siber saldırılarda zaman kısıtlaması olmadığı için ve tecrübeli bilgisayar korsanları tarafından gerçekleştirildiğinden dolayı keşif aşamalarında dikkat çekecek kadar ağ trafiği oluşmayacaktır. Bundan dolayı gelişmiş siber saldırıları geleneksel yöntemler ile tespit etmek ve engellemek mümkün olmamaktadır. Aktif siber savunma yaklaşımında ise bu soruna karşı, saldırganları aldatma ve yavaşlatmaya yönelik çözümler önerilmektedir.

Siber ölüm zincirinin üçüncü fazı ile yedinci fazı arasında savunucular saldırıyı tespit etmek, saldırıyı engellemek, saldırganlar ve onların metotları hakkında bilgi toplamak, saldırganları yanlış tarafa yönlendirmek ve hatta gelecekteki saldırılara karşı onları caydırmak için kolayca ilk adımı atabilirler (Lachow 2013).

Saldırganlar hedef ağa sızma girişimine başladığından itibaren ve kalıcılığı sağlayıncaya kadar geçen aşamada yani üçüncü, dördüncü ve beşinci fazlarda çalışma yaptıkları zaman tespit edilmeleri ilk iki faza göre daha kolay ve mümkün olsa bile kullandıkları gelişmiş ve yeni tekniklerden dolayı yakalanma ihtimalleri düşüktür. İmza tabanlı güvenlik sistemleri gibi geleneksel savunma sistemleri ile yakalanmaları neredeyse

imkânsızdır. Çünkü saldırganların kullandığı yeni teknik ile ilgili henüz bir imza mevcut olmayacaktır. Bu duruma çözüm olarak aktif siber savunma konseptine uygun olarak Vaarandi (2013) tarafından yapılan çalışmada insanların yazdığı imza veri tabanına güvenmek yerine ağ trafiğini normal ve anormal olarak sınıflandırmak için çeşitli algoritmalar kullanan ağ izleme yöntemleri önerilmiştir.

Lachow (2013)'un belirttiğine göre, kurulan zararlı yazılım işletmenin dışı ile iletişime başladığında, yani faz 6 (komuta ve kontrol)'da organizasyonlar saldırıyı bozmak için ne yapacaklarını bilmemektedir.

Siber ölüm zincirinin yedinci aşamasında ise amaca göre eylem vardır. Artık saldırgan iç ağdadır ve amacına yönelik faaliyetler yapmaktadır. Yaşanmış örneklere bakıldığında kurbana ait politik, ekonomik, askeri vb. kritik konular ile ilgili veri çalmak olduğu görülmektedir. Bundan dolayı bu aşamada yapılacak aldatma faaliyetleri önemlidir. Aldatma teknikleri yavaşlatma, saldırganı ele geçirme ve yanlış bilgileri ele geçirmesini sağlama gibi amaçlar için kullanılabilir.

Balküpleri kurarak ağı olduğundan büyük göstermek ve bal küpleri üzerinde gereksiz servisleri çalıştırmak saldırganın keşif aşamasında işini zorlaştıracaktır. Doğru tespit için daha fazla tarama yapması gerekecektir. Balküpü ile yapılabilecek bir diğer saldırı yöntemi ise zararlı dokümanların saldırgan tarafından çalınmasını sağlamaktır. Bu sayede zararlı yazılım bulaştırılan saldırgan ağı ele geçirilebilir.

4.3 ACD Yöntemlerinin Siber Saldırılara Karşı Etkisinin İncelenmesi

Bu çalışmanın amacı, karşı atak, yavaşlatma, aldatma gibi aktif siber savunma kapsamında ele alınan yöntemlerin uygulamasında kullanılabilecek DOS/DDOS saldırısı ve ADHD üzerindeki Spidertrap, Portspoof ve BeEF gibi araçlarının uygulamadaki etkinliğinin ölçülmesidir. Bu amaçla kurulan laboratuvarda aktif siber savunma yaklaşımının karşı atak, yavaşlatma ve aldatma yaklaşımına yönelik testler yapılacaktır ve test sonuçları tartışılacaktır.

Siber saldırılarda farklı yöntemler ile sistemlerin ele geçirilmesi amaçlanır. Bu

yöntemler bazen sistemlerdeki açıklıkların sömürülmesi, bazen sosyal mühendislik saldırısı yöntemleri ile kullanıcı bilgisayarlarına zararlı yazılım bulaştırılması gibi yöntemler olarak ortaya çıkar.

Gelişmiş siber saldırıların normal siber saldırılardan bir farkı da sıfırıncı gün açıklığı, olarak adlandırılan zararlı yazılımlar kullanılması olduğu belirtilmişti. Bundan dolayı kurulan laboratuvarda kullanılan zararlı yazılımların test esnasında IDS/IPS sistemlerine yakalanması durumunda uyarı göz ardı edilecektir.

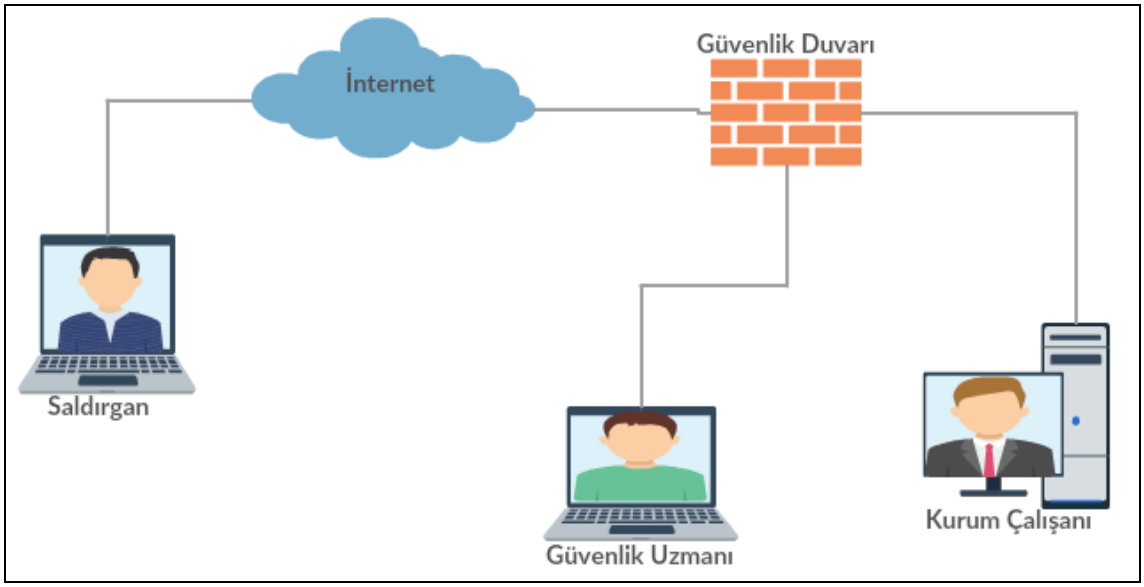
Laboratuvar ortamında kullanılacak makineler ve teknik özellikleri:

- pfSense güvenlik duvarı: ücretsiz açık kaynak kodlu FreeBSD tabanlı güvenlik duvarı, 1552MB (1.5GB) RAM, 2 işlemcili, 10 GB SSD depolama alanı,
- Saldırgan makinesi: Linux tabanlı işletim sistemi Ubuntu dağıtımı, 3072 MB (3GB) RAM, 20 GB SSD depolama alanı,
- Güvenlik uzmanının makinesi: Gelişmiş Penetrasyon Testi Linux dağıtımı, 3328 MB (3GB) RAM, 50 GB SSD depolama alanı
- Balküpü makinesi: Debian 7 x64 (wheezy) işletim sistemi, 4 GB RAM, 50 GB SSD depolama, 2 işlemcili,
- Kurum çalışanının makinesi: Windows 7 işletim sistemi, 1024 MB(1GB) RAM, tek işlemcili, 20 GB SSD depolama alanı,

olacak şekilde tasarlanmıştır. Hassas ölçümler yapılmayacağından dolayı makinelerin teknik özellikleri arasındaki farklılıklar göz ardı edilmiştir. Ayrıca makineler test senaryosunda yapılacak saldırılar doğrultusundaki muhtemel performans ihtiyaçlarına göre tasarlanmıştır. Senaryolarda kullanılan ağ topolojileri sanallaştırma sistemi üzerine kurulmuştur.

4.3.1 DOS ve DDOS Saldırılarının Karşı Atak Etkisinin İncelenmesi

Yapılan ilk test denemelerinde karşı atak etkisi incelenecektir ve bu amaçla laboratuvarda Şekil 4.1'de gösterilen ağ yapısı kurulmuştur. Bu yapıda, A Kurumuna ait güvenlik duvarının arkasında bir son kullanıcı, bir güvenlik uzmanı vardır ve internet tarafında bulunan bir saldırgan vardır. Test senaryosu bölüm 4.3.1.1'de verilmiştir.



Şekil 4.1 Karşı atak denemelerinde kullanılan laboratuvarın ağ yapısı.

4.3.1.1 DOS ve DDOS Testi Senaryosu

Hedefteki kuruma sızmak isteyen saldırgan, yaptığı keşif ve zafiyet taramaları sonucunda sistemlerde açıklık tespit edemez. Bundan dolayı hedef olarak sistemin en zayıf halkası olan son kullanıcıları seçer. Son kullanıcı bilgisayarını ele geçirmek için kullanacağı zararlı yazılımı hazırlar. Saldırgan, kullanıcıya sosyal mühendislik saldırısı yaparak bu yazılımın hedef bilgisayarda kullanıcı tarafında çalıştırılmasını sağlar. Böylece saldırgan son kullanıcının bilgisayarını ele geçirmiştir. Bundan sonraki aşamada saldırgan ele geçirdiği makinede kalıcılığı sağlayıp ağdaki diğer sistemlere sızmayı hedefler.

Saldırganın kullandığı zararlı yazılım sıfırıncı gün açıklığı içeren bir yazılım olsaydı imza tabanlı kontrol yapan güvenlik sistemleri tarafından tespit edilmesi mümkün olmayacaktı. Ancak ağda zararlı yazılım analizi yapılması sonucu tespit edilebilirdi. Ayrıca kullanılan zararlı yazılım ya da saldırganın diğer sızma faaliyetleri bilgisayarda veya ağda yavaşlık vb. dikkat çekici, şüphe uyandırıcı bir duruma sebep olursa belki tespit edilebilirdi.

Test senaryosunda bilgisayarına zararlı yazılım bulaşan kullanıcı kurbanı olduğu sosyal mühendislik saldırısı sonrası internetinde oluşan yavaşlamadan şüphelenerek kurumun güvenlik uzmanından destek ister. Güvenlik uzmanı zararlı yazılım bulaşmış makinenin görev yöneticisinde (task manager) çalışan uygulamaları inceler. Ayrıca komut istemcisinde (cmd.exe) 'netstat –an' komutunu çalıştırarak bilgisayarın hangi IP adresleri ile bağlantı kurduğunu inceler. İnceleme sonrası bilgisayara bulaşan zararlı yazılımı ve saldırganın bağlantı kurduğu IP adresini tespit eder.

Güvenlik uzmanı ilk olarak tespit ettiği bu yabancı IP adresinin kimin adına kayıtlı olduğu vb. bilgileri 'www.whois.com' uygulaması üzerinden kontrol eder. Saldırının ve saldırganın tespit edilmesi sonrası kurumun güvenlik uzmanı güvenlik duvarına kural girerek saldırganın IP adresini engellemek yerine karşı atak denemeleri yaparak bu erişimi engellemeyi ve saldırganın ağına zarar vermeyi amaçlamaktadır. Ayrıca saldırganı korkutup daha sonra saldırı yapmasını engellemeyi hedeflemektedir.

Yukarıda anlatılan senaryo çerçevesinde, saldırıyı engellemek amacıyla DOS ve DDOS saldırıları yapılmıştır. Bu saldırılarda saldırganın ağ alt yapısı ve sunucularına yönelik saldırılar yapılmıştır. Saldırganın ağ alt yapısına yönelik saldırılar 'hping3' aracı ile yapılmıştır. Bu saldırılar tek bir kaynak IP adresi üzerinden yapıldığında DOS saldırısı, birden çok kaynak IP adresi üzerinden yapıldığında DDOS saldırıları olarak adlandırılır. Ancak laboratuvar ortamında yapılan testlerde IP spoof (aldatma) tekniği kullanılarak kaynak IP adresi birden çok farklı yerden geliyor gibi gösterilmiştir ki bu yöntemin işe yaradığı sızma testleri kapsamında yapılan DDOS testlerinde görülmüştür. Saldırganın bağlantı kurduğu sunucuya yönelik saldırılarda ise 'ab, httpflooder ve slowloris' gibi sunucu kaynaklarını tüketme saldırısı yapan araçlar kullanılmıştır. Örnek olarak, sırasıyla Şekil 4.2 ve Şekil 4.3'te hping3 aracı ile DOS ve DDOS saldırılarının nasıl yapıldığı gösterilmiştir. Bunlara ilaveten, burada göz ardı edilmemesi gereken bir nokta hping3 aracının varsayılan şekilde kurulduğunda IP aldatması (spoofing) özelliğini desteklemediği için yamalı (patch) halinin kullanılmış olmasıdır.

```
root@GuvenlikUzmani:~# hping3 -S --flood -p Saldirganin_Portu Saldirganin_IP_Adresi
```

Şekil 4.2 Hping3 aracı ile DOS saldırısı yapma.

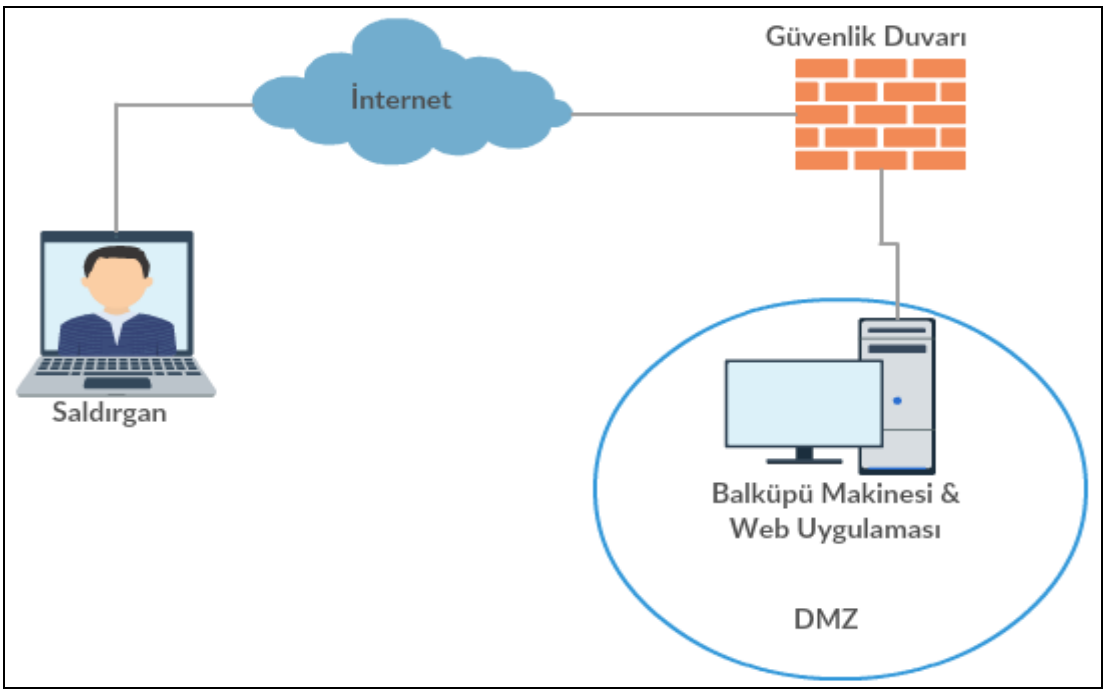
```
root@GuvenlikUzmani:~# hping3 -S --flood -p Saldirganin_Portu Saldirganin_IP_Adresi --rand-pattern-source Spoof_Edilecek_Ag_Adresi
```

Şekil 4.3 Hping3 aracı ile DDOS saldırısı yapma.

4.3.2 Active Defense Harbinger Distribution'nin (ADHD) Aktif Siber Savunmada Kullanılması

ADHD Ubuntu LTS tabanlı Linux dağıtımıdır. Bu dağıtım üzerine, aktif siber savunma amacıyla kullanılabilecek birçok araç kurulmuştur ve kullanıma hazır şekilde gelmektedir. Bu dağıtımın amacı, savunma tarafındaki güvenlik uzmanlarına, bilgisayar korsanlarına karşı atak yaparken yardımcı olmasıdır. Bu dağıtım üzerindeki araçların saldırganlar hakkında bilgi toplamadan, saldırganların sistemlerine zarar vermeye kadar bir sürü fonksiyonu vardır (İnt.Kyn.13).

Testin bu aşamasında ADHD dağıtımı üzerindeki araçların aktif savunmaya nasıl faydalı olabileceği araştırılmıştır ve bunu anlamaya yönelik uygulamalar yapılmıştır. Bu amaç ile Şekil 4.4'te gösterilen ağ topolojisi kurulmuştur. Kolay analiz edebilmek amacıyla saldırgan hakkında bilgi toplama, saldırganı yavaşlatma ve karşı atak olmak üzere üç ayrı senaryo üzerinde çalışılmıştır.



Şekil 4.4 Testin ikinci aşamasında kullanılan ağ topolojisi.

4.3.2.1 Saldırganlar Hakkında Bilgi Toplama Test Senaryosu

Diğer alanlarda yapılan saldırılarda olduğu gibi siber saldırılarda da saldırgan hakkında bilgi toplamak ve saldırganı tanımak önem arz etmektedir. Bu bilgiler siber saldırılara karşı önlem alırken ve saldırıya karşı cevap verirken kullanılabilir.

Saldırgan hakkında bilgi toplamak amacıyla ADHD üzerinde bulunan Honey Badger uygulaması kullanılmıştır. Bu uygulama ile saldırganın fiziksel konumu tespit edilmeye çalışılır. Bu tespiti yaparken de kullanıcıların tarayıcısındaki konum bilgisi paylaşma, görünebilir kablosuz ağları kullanma ve IP adresi bilgisini kullanma gibi jeolojik teknik bileşimlerini kullanmaktadır.

Bu senaryoda saldırganın kurum hakkında bilgi toplamak amacıyla yaptığı taramalar sonucu tespit ettiği DMZ (demilitarized zone-sivil bölge) bölgesinde bulunan balküpü sunucusunun web sayfasını ziyaret ettiği kabul edilir. Normal kullanıcılar kurumun bilinen web sayfasını, o sayfaya ait DNS adını kullanarak ziyaret ederler, ancak saldırganlar ise o kurumun ağındaki IP adreslerini tespit eder ve DNS adı ile bilinen web uygulamaları dışında bu IP adreslerinde çalışan sunucuları ve servisleri tespit ederler. Bundan dolayı sunucu üzerinde kurumun test aşamasındaki bir web uygulaması görünümünde olan balküpü sunucusunu ziyaret eder. Saldırganın bu sayfayı ziyaret etmesi sonucu web uygulamasının arka planında Honey Badger aracına yönelik bir web isteği yapar ve Honey Badger Şekil 4.5'te gönderilen cevabı döner ve bunun sonucu olarak saldırganın tarayıcısında konum paylaşma ve javascript kodu çalışma isteği oluşur.

```
<!doctype html>
<head>
<script type="text/javascript" src="honey.js"></script>
<!--<meta http-equiv="refresh" content="0; url=http://149.202.232.129/" /> -->
</head>
<body>
<h1>Welcome...! :))</h1>
<img src="service.php?target=Demo_Page&agent=HTML" onerror="go('/honeybadger/service.php',
'Demo_pages','honey.jar',true,true,false,5000);" width="1px" height="1px" />
</body>
</html>
```

Şekil 4.5 Honey Badger tarafından cevap olarak verilen HTML kodu.

4.3.2.2 Saldırganı Yavaşlatma Test Senaryosu

Testin bu aşamasında saldırganları yavaşlatmaya yönelik çalışmalar incelenmiştir. Bu kapsamda ADHD üzerindeki Spidertrap ve Portspoof araçları kullanılmıştır. Bu araçların savunmaya etkinliği ve kullanılabilirliği araştırılmıştır.

Spidertrap web uygulamasında iç içe dinamik dizinler oluşturur. Bu sayede web tarama araçlarının çalışmasını yavaşlatması amaçlanmaktadır. Test ortamında da bu etki incelenmiştir. Buna ilaveten bu aracın ziyaret edilen dizinleri kayıt altına alındığı göz önüne alınırsa ve uygulamanın kullandığı dizinler kurumun çalışma alanına yönelik bilgiler doğrultusunda tasarlanırsa hedefli saldırılar karşısında, saldırganın hedefindeki bilgilerin ne olduğunu anlamaya yönelik de kullanılabilir.

Spidertrap uygulaması çalıştırıldığında üzerinde bulunduğu sunucunun 8000. portu üzerinden yayın yapar. Balküpü olarak hazırlanan web uygulamasına yerleştirilen kodlar ile saldırganın istekleri buraya yönlendirilir. Bu test senaryosunda Şekil 4.4'te gösterilen ağ topolojisinde balküpü amacıyla kurulan web uygulamasına yönelik otomatik tarama araçlarıyla tarama yapılmıştır. İlk taramada Spidertrap uygulaması devre dışı bırakılmış ve taramanın ne kadar sürede gerçekleştiğine bakılmıştır. Daha sonra Spidertrap uygulaması balküpü üzerinde aktif hale getirilip ve yine aynı tarama yapılmıştır. Bu iki tarama sonucu analiz edilerek Spidertrap aracının yavaşlatma konusunda etkinliği incelenmiştir. Uygulamaya yönelik tarama saldırganların ve güvenlik uzmanlarının kullandığı saldırı araçlarıyla özelleştirilmiş Kali Linux işletim sistemi üzerindeki ücretsiz tarama araçlarıyla yapılmıştır.

Portspoof aracı saldırganların keşif çalışmalarını yavaşlatmak amacıyla geliştirilmiş bir araçtır. Saldırganlar tarafından işletim sistemine yönelik yapılan taramalarda tüm portlar açık ve üzerinde servis çalışıyor gibi cevap dönerek saldırganların port kapalı ya da filtreli cevabı alması yerine port açık bilgisi almasını sağlar. Bu sayede saldırganların yanlış bilgi toplamasını sağlarken taramanın da yavaş olmasını sağlamaya çalışır. Yavaşlatmaya yönelik yapılacak diğer test aşamasında Portspoof aracının yavaşlatmaya yönelik etkisi incelenmiştir.

Portspoof aracı kurulu olduğu balküpünün 4444. portu üzerinde yayın yapar ve örnek olarak Şekil 4.6'da gösterildiği şekilde aldatılmak istenen portların 4444 portuna yönlendirilmesi sonrası, yönlendirilen porta gelen isteğe Portspoof aracı cevap döner.

```
# iptables -t nat -A PREROUTING -i eth0 -p tcp -m tcp --dport 1:65535 -j REDIRECT --to-ports 4444
```

Şekil 4.6 Tüm portların 4444 portuna yönlendirilmesi.

Portspoof aracı için uygulanacak test senaryosu da bir önceki senaryoya benzerdir ve ağ topolojisi Şekil 4.4'te gösterildiği şekildedir. İlk olarak Portspoof aracı kapalı iken ağ keşif aracı (network mapper – Nmap) ile tarama yapılmıştır. Daha sonra Portspoof aracı aktif durumdayken tarama yapılmıştır ve sonuçlar karşılaştırılarak analiz edilmiştir. Bu iki durum için iki tarama gerçekleştirilmiştir. Birinci taramada Şekil 4.7'de gösterilen tarama yapılmıştır ve tüm portlar taranmıştır. İkici taramalarda ise Şekil 4.8'de gösterilen tarama yapılmıştır ve açık portlara ilaveten bu portlar üzerinde çalışan servisler de tespit edilmeye çalışılmıştır. Servis tespit taramaları daha uzun sürdüğü için 1. Port ile 1000. Port arası taranmıştır.

```
root@hacker:~# nmap -sS -n -Pn 149.202.232.129 -p1-65535 -oN tarama1
```

Şekil 4.7 Birinci tarama.

```
root@hacker:~# nmap -sS -sV -n -Pn 149.202.232.129 -p1-1000 -oN tarama2
```

Şekil 4.8 İkinci tarama.

Şekil 4.7 ve Şekil 4.8'de görülen taramalar, ağ keşif çalışmalarında kullanılan Kali Linux üzerinde de bulunan Nmap ağ tarama aracı ile yapılmıştır.

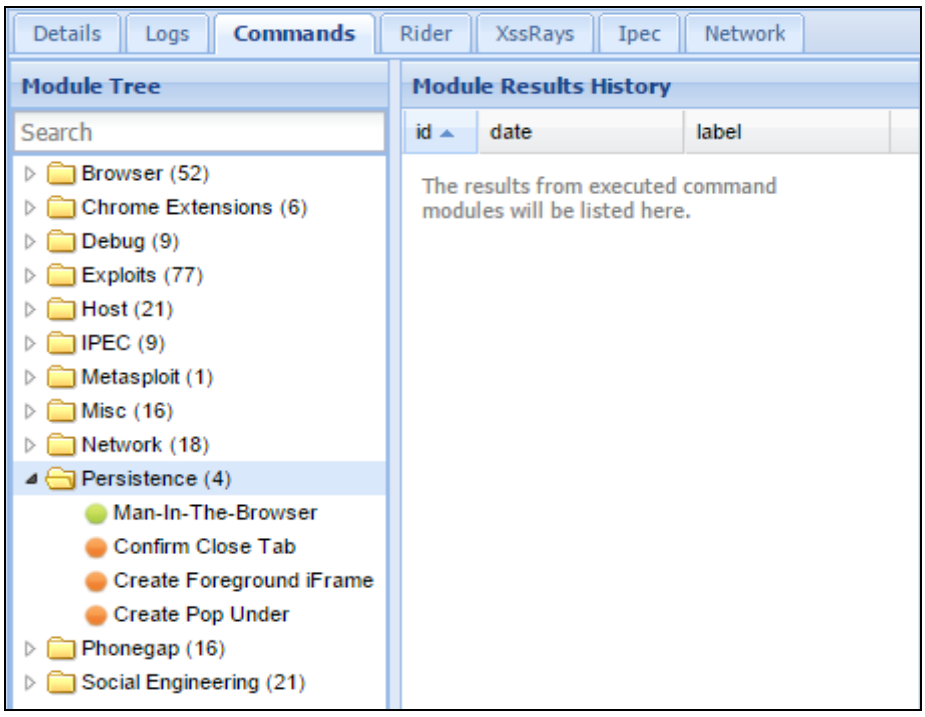
4.3.2.3 Karşı Atak Test Senaryosu

Karşı atak test senaryosunda yine Şekil 4.4'te gösterilen ağ topolojisi kullanılmıştır. Balküpü sunucusu üzerinde çalışan uygulamanın arka planında karşı atak için BeEF aracı kullanılmıştır. BeEF aracı tarayıcı sömürme çerçeve projesi (The Browser Exploitation Framework Project) olarak geliştirilmiştir. BeEF, kurbanlarının

tarayıcılarını ele geçirmek için javascript kodu kullanır.

Test senaryosu şu şekildedir; balküpü üzerinde çalışan web uygulaması, saldırgan bu uygulamayı ziyaret ettiğinde arka planda otomatik olarak javascript kodu olan sayfası ziyaret etmesini sağlayacak şekilde, tasarlanmıştır. Bundan dolayı kurum ağını keşfetmeye çalışan saldırganın bu sayfayı ziyaret etmesi sonucu tarayıcısının ele geçirilmesi amaçlanır.

BeEF aracı üzerinde farklı saldırıları gerçekleştirmeye yönelik modüller vardır. Bu modüller Şekil 4.9'da gösterilmiştir. Saldırganın tarayıcısı ele geçirildikten sonra BeEF aracı üzerinde modüller kullanılarak saldırı ilerletilebilir. Bu test senaryosunda örnek olarak saldırganın makinesi üzerindeki açık portlar ve yerel ağında bulunan cihazlar hakkında bilgi toplanmaya çalışılmıştır.

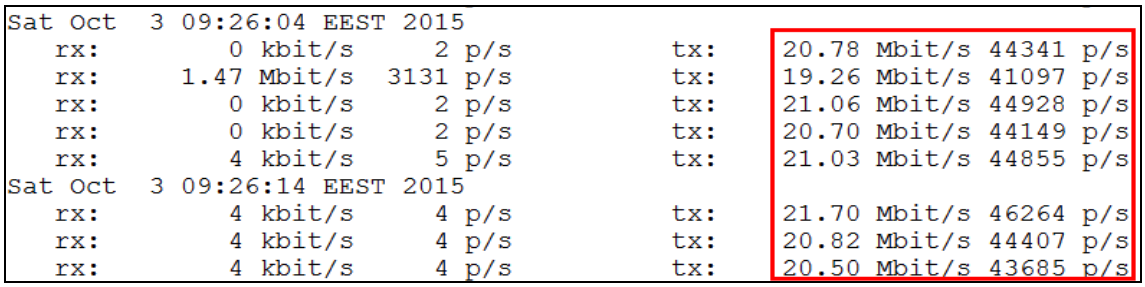


Şekil 4.9 BeEF aracı üzerindeki saldırı modülleri.

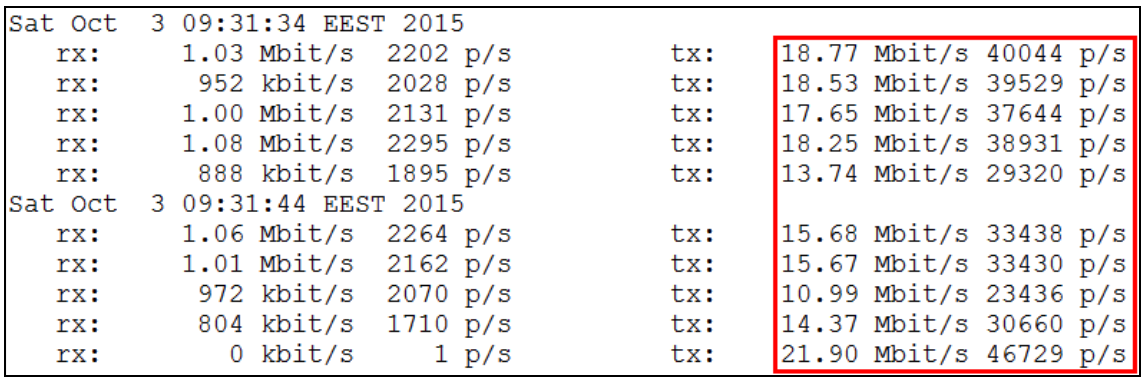
5. BULGULAR

5.1 DOS ve DDOS Testi Sonucu

Saldırganın ağ alt yapısına yönelik yapılan testlerde beklenen sonuç elde edilememiştir. Bu durumun nedeni laboratuvar alt yapısının sanallaştırma sistemi ile tek bir fiziksel sunucu üzerine kurulmuş olmasıdır. Bundan dolayı yeterince yüksek bant genişliğinde saldırı yapılamamıştır. Şekil 5.1 ve Şekil 5.2'de 'de test ortamında DOS ve DDOS saldırılarında ne kadar bant genişliğinde (bandwith) saldırı yapıldığı sırasıyla gösterilmiştir.



Şekil 5.1 Test ortamında DOS saldırısı esnasında ulaşılan bant genişliği.



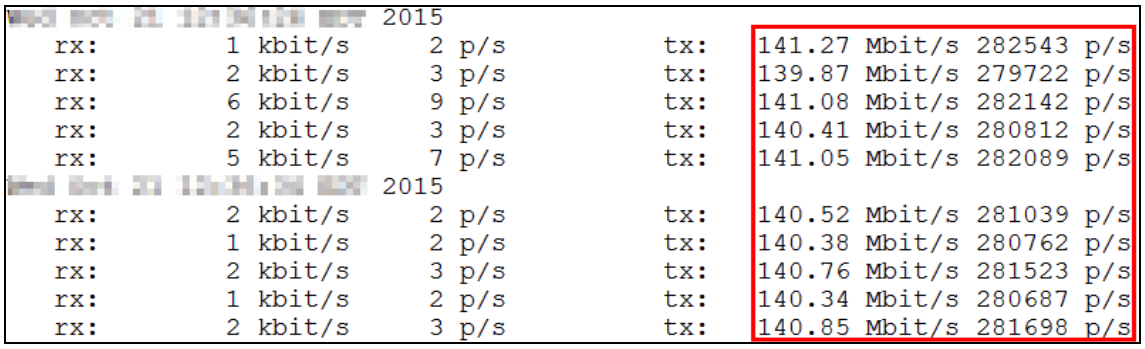
Şekil 5.2 Test ortamında DDOS saldırı esnasında ulaşılan bant genişliği.

Ulaşılan bant genişliği 'vnStat' aracı ile ölçülmüştür. 'vnStat', Linux ve BSD tabanlı işletim sistemleri için konsol tabanlı ağ trafiğini izlemek için geliştirilmiştir (İnt.Kyn.17). Bu araç ile saldırı esnasında ne kadar büyüklükte bir bant genişliğinde saldırı yapıldığı gözlemlenebilir.

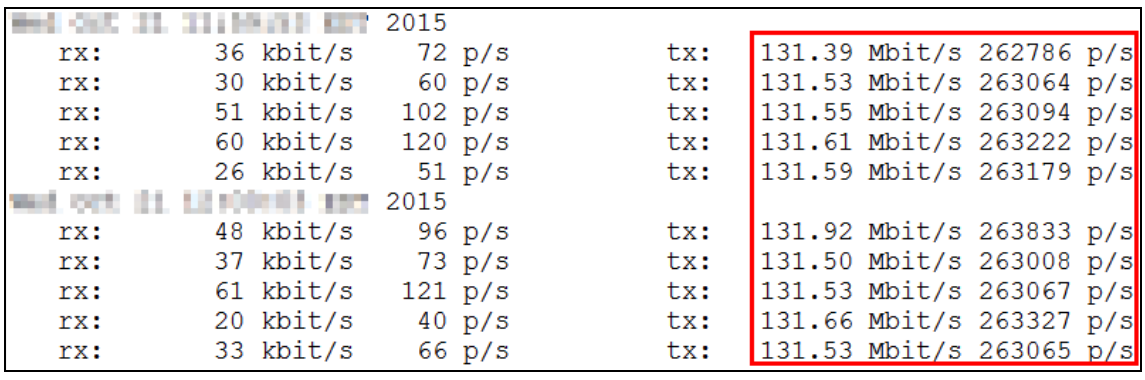
Saldırganın sunucusuna yönelik yapılan testlerde ele geçirdiği bilgisayar ile arasındaki

bağlantının kopmadığı ancak iletişimin yavaşladığı görülmüştür. Ayrıca testin tutarlılığını gözlemlemek amacı ile yapılan tekrar testlerinde de sonucun değişmediği gözlemlenmiştir.

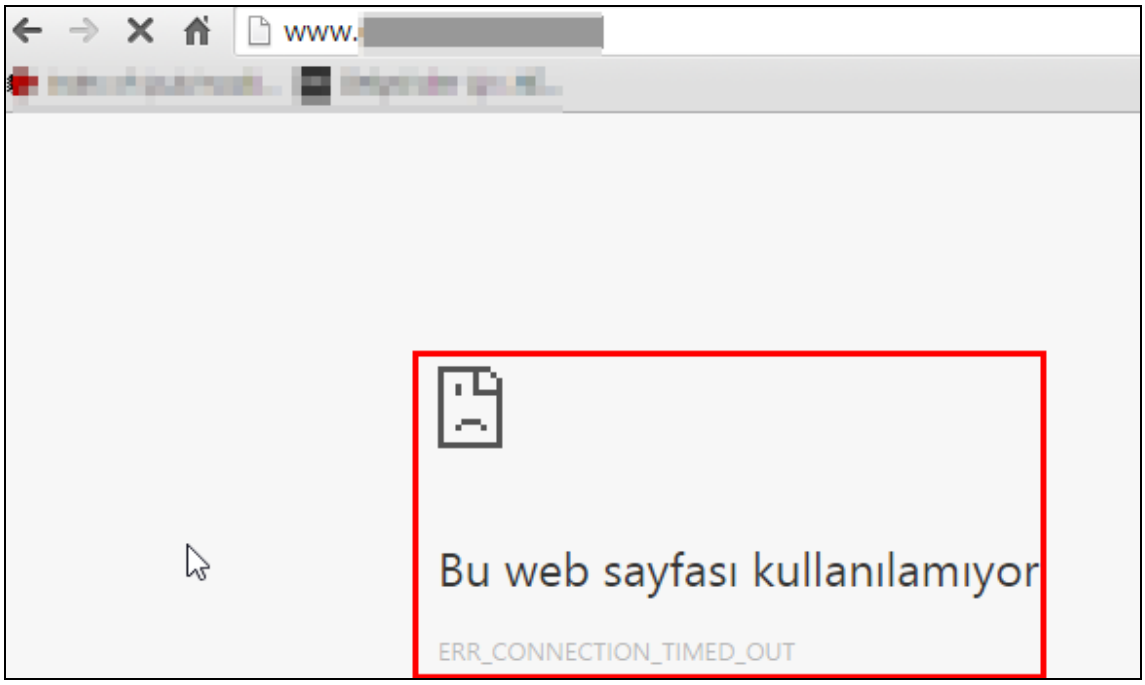
Gerçek ağlara yönelik daha önce yapılan sızma testlerinde, DOS ve DDOS saldırılarının iç ağ altyapısını dahi etkilediği görülmüştür. Buna ilaveten ağ alt yapısına yönelik yapılan DOS ve DDOS testlerinde saldırının başarılı olup olmayacağını saldırgan taraf ile kurbanın bant genişliği etkileyen faktördür. Şekil 5.3 ve Şekil 5.4'te örnek olarak gerçek bir DOS ve DDOS saldırısında ulaşılan bant genişliği sırasıyla gösterilmiştir. Ayrıca sunuculara yönelik yapılan DOS ve DDOS testlerinde eğer sunucuda gerekli güvenlik önlemleri alınmaz ise sunucunun çalışamaz hale geldiği de gözlemlenmiştir. Örnek olarak Şekil 5.5'te gerçek bir saldırıda cevap veremez hale gelmiş bir uygulama sunucusunun ekran görüntüsü gösterilmiştir.



Şekil 5.3 Gerçek ortamda DOS saldırısı esnasında ulaşılan bant genişliği.



Şekil 5.4 Gerçek ortamda DDOS saldırı esnasında ulaşılan bant genişliği.



Şekil 5.5 Gerçek bir saldırıda isteklere cevap veremez hale gelmiş sunucu.

Servis dışı bırakma saldırılarının yeterli kaynaklar sağlanması durumunda başarısız olmasının neredeyse imkânsız olabileceği savunulabilir. En ütopik senaryo olarak gelişmiş bir DOS/DDOS koruma sisteminin karşısına daha güçlü ve henüz kara listeye eklenmemiş bir botnet ile çıkıldığında saldırının başarılı olma ihtimali muhtemeldir. Ancak diğer alanlarda yapılan çalışmalarda olduğu gibi siber güvenlik alanında yapılan çalışmalarda da teoride veya test ortamında yapılan çalışmalar ile gerçek ortamda yapılan çalışmalar arasında uygulama sorunları ya da farklılıkları ortaya çıkabilmektedir. Yani her aşama anlatıldığı kadar kolay ve uygulanabilir olmayabilir. DOS ve DDOS testlerinin etkinliğini ölçmek için laboratuvar ortamında yapılan deneylerde saldırganın kısmen yavaşlatılabildiği gözlemlenmiştir. Ancak etkili sonuçları olan DOS ve DDOS testlerini saldırgana karşı uygulamak her zaman kolay olmayabilir. Bu senaryo ele alınıp ne gibi eksikler olabilir diye bakıldığında ortaya bazı engeller çıkmaktadır.

İlk olarak saldırının tespit edilmesine değinmek gerekirse, gerçek saldırılarda ki özellikle tecrübeli bir saldırgan tarafından yapılan bir saldırıda bilgisayarı ele geçirilen kurbanın bunu fark etmesi kolay olmamaktadır. Sızma testleri kapsamında gerçek ortamda yapılan çalışmalarda da bu durum görülmüştür. Ayrıca büyük kurumların ağ

trafiği de yüksek olduğu için güvenlik uzmanları tarafından düzenli ve sistemli olarak izlenmeyen ağlarda sızma girişimini veya sızmayı tespit etmek kolay değildir.

Bu senaryodaki eksik nokta ise saldırganın doğrudan kendi IP adresi üzerinden geldiği varsayımıdır. Eğer burada saldırgan kendi ağı üzerinden değil de ele geçirdiği bir başka kurban üzerinden saldırı gerçekleştirseydi karşı atak yapmak teknik ve hukuki açıdan çok kolay olmayacaktı. İşin hukuki boyutu bir kenara bırakılıp teknik taraf ele alındığında ortaya şöyle bir sorun çıkmaktadır. Eğer saldırının geldiği IP adresine karşı atak yapılırsa saldırgana zarar vermekten çok bir başka ağa zarar vermiş olunurdu. Bu kurum sağlık, ekonomi, ulaşım vb. kritik görev üstlenen bir kurum ise bu kurumlar hizmet veremez hale gelebilir ve bundan dolayı saldırgana zarar vermekten çok kamu kurumlarına zarar vermiş olunurdu.

Ağın bant genişliği ve saldırı yapılan sunucunun performansı dikkate alındığında, eğer saldıranın bant genişliği kurbanınkinden büyükse ya da saldırganının sunucusu daha performanslı ise bu senaryoda yapılan karşı atak denemesi işe yaramayacaktır.

5.2 Saldırganlar Hakkında Bilgi Toplama Testi Sonucu

Testlerde Honey Badger uygulaması tarafından saldırganın tarayıcısında oluşan, konum bilgisi paylaşma ve tarayıcısında javascript çalıştırma isteklerine verdiği olumlu ve olumsuz cevap senaryoları ve bunlar sonucunda elde edilen bilgiler incelenmiştir. Şekil 5.6'da saldırganın konum bilgisini paylaşma isteğine olumlu cevap vermesi sonucu elde edilen bilgiler görülmektedir.

```
[10/13/2015 23:32:42] [*] ================================================
[10/13/2015 23:32:42] [*] Connection from Demo_Page @ 88.230.51.223:49244 via HTML
[10/13/2015 23:32:42] [*] Query String: target=Demo_Page&agent=HTML
[10/13/2015 23:32:42] [*] User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:41.0)
Gecko/20100101 Firefox/41.0
[10/13/2015 23:32:42] [*] Comment:
[10/13/2015 23:32:42] [*] Attempting to geolocate by IP.
[10/13/2015 23:32:44] [*] API URL used: http://uniapple.net/geoip/?ip=88.230.51.223
[10/13/2015 23:32:44] [*] JSON object retrived:
{"country":"TR","region":"61","city":"Trabzon","postal_code":"NULL","latitude":"41.0050",
"longitude":"39.7269","metro_code":"0","area_code":"0"}
[10/13/2015 23:32:44] [*] Target location identified as Lat: 41.0050, Lng: 39.7269
```

Şekil 5.6 Saldırganın Konum Paylaşma İsteğine Olumlu Cevap Vermesi ile Elde Edilen Bilgiler.

Şekil 5.6'da görüldüğü üzere saldırganın IP adresi, kullandığı tarayıcı bilgisi ve jeolojik konum bilgisi elde edilmiştir. Bu bilgiler kullanılarak saldırgana yönelik yapılacak saldırılarda aksiyon alınabilir. Örnek vermek gerekirse saldıranın makinesi ele geçirilmek istenirse Mozilla Firefox uygulamasına yönelik bir zafiyet kullanılabilir.

Şekil 5.7'de saldırganın javascript kodu çalıştırma isteğine olumlu ancak konum paylaşma isteğine olumsuz cevap vermesi sonucu elde edilen bilgiler görülmektedir. Bu senaryoda göz ardı edilmemesi gereken bir nokta saldırganın makinesinde aktif kablosuz ağ kartı olduğu varsayımıdır.

```
[10/13/2015 23:33:25] [*] ================================================
[10/13/2015 23:33:25] [*] Connection from Demo_pages @ 88.230.51.223:49249 via Applet
[10/13/2015 23:33:25] [*] Query String: POST
[10/13/2015 23:33:25] [*] User-Agent: Mozilla/4.0 (Windows 8.1 6.3) Java/1.8.0_60
[10/13/2015 23:33:25] [*] Comment
[10/13/2015 23:33:25] [*] Input filtered: U1NJRCAxIDogVmlyZWxlcy...
[10/13/2015 23:33:25] [*] Data received: U1NJRCAxIDogVmlyZWxlcyA...
[10/13/2015 23:33:25] [*] Decoded Data: SSID 1 : Vireles BSSID 1:90:f6:52:7b:b6:dc Signal: 83%
SSID 2:ZyXEL BSSID 1: 00:02:cf:8d:44:c2 Signal: 26%BSSID 2
[10/13/2015 23:33:25] [*] API URL used: https://maps.googleapis.com/maps/api/browserlocation
/json?browser=firefox&sensor=true&wifi=mac:90:f6:52:7b:b6:dc|ssid:Vireles|ss:-17&
wifi=mac:00:02:cf:8d:44:c2...
[10/13/2015 23:33:25] [*] JSON object retrived:
{
   "accuracy" : 50,
   "location" : {
      "lat" : 39.9140502,
      "lng" : 32.8609375
   },
   "status" : "OK"
}
```

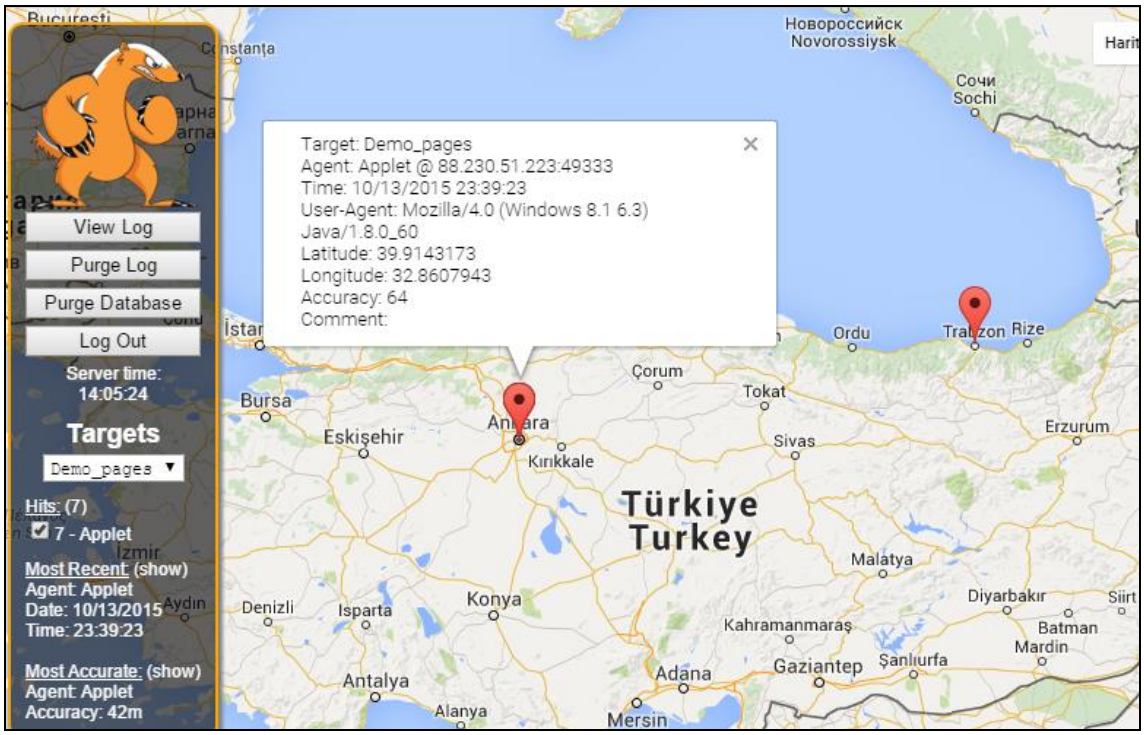
Şekil 5.7 Saldırganın javascript kodu çalıştırılması isteğine olumlu cevap vermesi ile elde edilen bilgiler.

Şekil 5.7'de görüldüğü üzere saldırgan tarayıcısında çalışan javascript kodunun kablosuz ağ kartını kullanarak etraftaki kablosuz ağlar hakkında bilgi topladığı görülmüştür. Ayrıca yine tarayıcı bilgisinin de elde edildiği görülmüştür.

Saldırganın konum paylaşma isteğine ve javascript kodu çalıştırılması isteğine olumlu cevap vermesi durumunda ise Şekil 5.6 ve Şekil 5.7'de gösterilen bilgilerin ikisinin de elde edildiği görülmüştür.

Honey Badger uygulaması yukarıda gösterilen şekilde elde edilen konum bilgilerini kullanarak saldırganların konumlarını harita üzerinde de göstermektedir. Örnek olarak

Şekil 5.8'de iki saldırganın harita üzerindeki konumu gösterilmiştir.

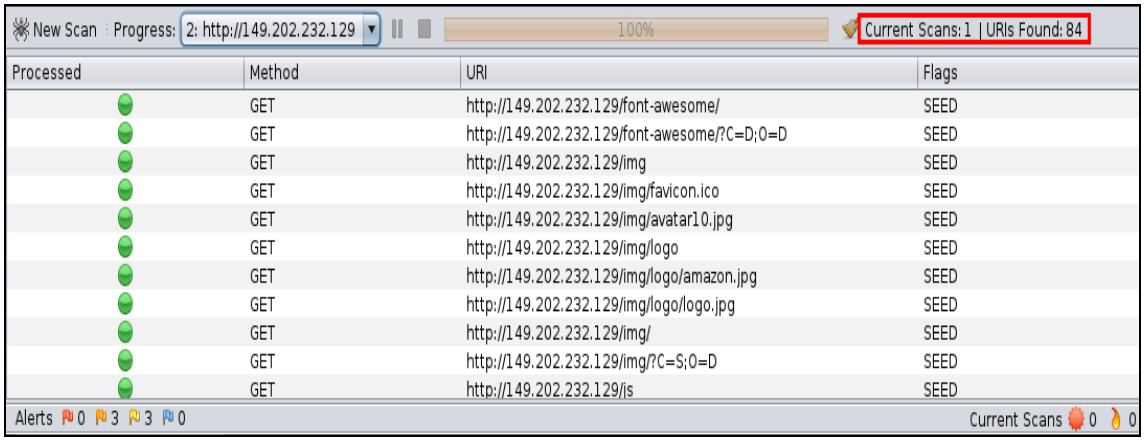


Şekil 5.8 Saldırganların harita üzerinde konumlarının gösterilmesi.

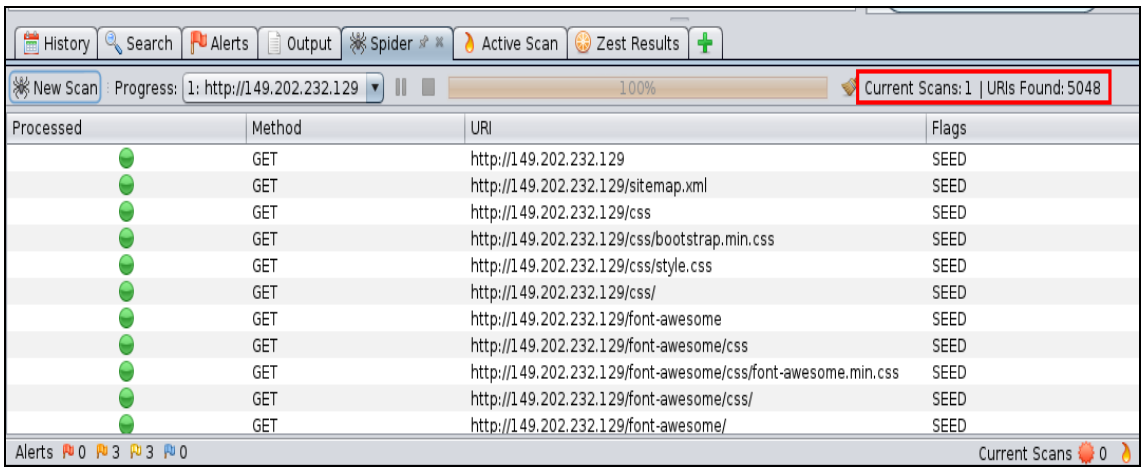
Honey Badger aracı ile yapılan testlerde, bu araç sayesinde saldırganın saldırıya yönelik verdiği tepkiye göre saldırgan hakkında bilgi toplanabildiği tespit edilmiştir. Saldırganın sayfayı ziyaret etmesi sonrası IP adresinden fiziksel konumuna, tarayıcı bilgisinden fiziksel çevresindeki kablosuz ağlar hakkında bilgi toplanabildiği gözlemlenmiştir.

5.3 Saldırganı Yavaşlatma Testi Sonucu

Spidertrap uygulamasının yavaşlatmaya etkisini incelemek için Kali Linux üzerindeki OWASP ZAP aracı ile tarama yapılmıştır. Sonuç olarak, Spidertrap aracı kapalıyken, web uygulamaya yönelik yapılan taramanın yaklaşık 1 dakika gibi kısa bir sürede tamamlandığı ve uygulama üzerinde 84 tane URL tespit edildiği görülmüştür. Buna karşılık, aynı web uygulamasının arka planında Spidertrap aracı çalışırken yapılan taramanın yaklaşık 33 dakika sürdüğü ve toplamda uygulama üzerinde 5048 tane URL tespit edildiği görülmüştür. Tarama sonuçlarının çıktısı test sırasına göre Şekil 5.9 ve Şekil 5.10'da verilmiştir.



Şekil 5.9 Spidertrap uygulaması kapalıyken yapılan taramanın sonucu.



Şekil 5.10 Spidertrap uygulaması açıkken yapılan taramanın sonucu.

Spidertrap aracı ile yapılan testlerde kullanılan otomatik tarama aracının ne kadar yavaşlatabildiği ölçülmüştür. Yapılan testler sonucunda Spidertrap uygulamasının Kali Linux üzerindeki OWASP ZAP uygulaması karşısında başarılı olduğu ve taramayı yavaşlattığı tespit edilmiştir. Ancak aynı test daha performanslı çalışan ücretli araçlar ile yapıldığında sonucun bu kadar etkili olmadığı görülmüştür. Bu durumun iki nedeni olabileceği tahmin edilmektedir. Birincisi, ücretli tarama araçlarının daha profesyonel uygulamalar olması sebebiyle balküpü gibi uygulamaları tespit edip, kullandığı tarama teknikleri sayesinde atlatmaya yönelik bir özelliği olabilir. İkicisi, ücretli uygulamalar daha performanslı olabileceği için laboratuvar ortamında yapılan deneylerde aradaki yavaşlama farkı gözlemlenememiş olabilir. Ayrıca bu laboratuvar ortamında kısıtlı imkânlardan dolayı, saldırgan profilini çıkarma ve hedefinin ne olduğunu anlamaya yönelik çalışma yapma imkânı olmamıştır. Eğer daha geniş bir ağ ortamında bu deney

yapılsaydı ve burada hedef kurum ve çalışma kapsamına yönelik dizinler oluşturulabilseydi deneyden daha etkili sonuç elde edilebilirdi.

Portspoof aracının yavaşlatmaya yönelik etkisini ölçmek için yapılan birinci tarama testinin sonuçları, Portspoof kapalıyken ve Portspoof açıkken olmak üzere sırasıyla Şekil 5.11 ve Şekil 5.12'de verilmiştir.

```
# Nmap 6.47 scan initiated Fri Oct  2 13:01:25 2015 as: nmap -sS -n -Pn -p1-65535 -oN tarama1_1 149.202.232.129
Nmap scan report for 149.202.232.129
Host is up (0.52s latency).
Not shown: 65521 closed ports
PORT      STATE    SERVICE
25/tcp    filtered smtp
80/tcp    open     http
111/tcp   open     rpcbind
445/tcp   filtered microsoft-ds
2000/tcp  open     cisco-sccp
3000/tcp  open     ppp
3389/tcp  open     ms-wbt-server
8000/tcp  open     http-alt
53009/tcp open     unknown
61985/tcp open     unknown
61986/tcp open     unknown
64322/tcp open     unknown
64380/tcp open     unknown
64381/tcp open     unknown

# Nmap done at Fri Oct  2 13:38:45 2015 -- 1 IP address (1 host up) scanned in 2240.21 seconds
```

Şekil 5.11 Portspoof aracı kapalıyken yapılan taramanın sonucu.

```
# Nmap 6.47 scan initiated Fri Oct  2 11:53:08 2015 as: nmap -sS -n -Pn -p1-65535 -oN tarama1_2
Nmap scan report for 149.202.232.129
Host is up (0.40s latency).
PORT      STATE    SERVICE
1/tcp     open     tcpmux
2/tcp     open     compressnet
3/tcp     open     compressnet
4/tcp     open     unknown
5/tcp     open     unknown
6/tcp     open     unknown
7/tcp     open     echo
8/tcp     open     unknown
9/tcp     open     discard
10/tcp    open     unknown
11/tcp    open     systat
12/tcp    open     unknown
13/tcp    open     daytime
14/tcp    open     unknown
15/tcp    open     netstat
16/tcp    open     unknown
17/tcp    open     qotd
18/tcp    open     unknown
  ...       ...        ...
65528/tcp open     unknown
65529/tcp open     unknown
65530/tcp open     unknown
65531/tcp open     unknown
65532/tcp open     unknown
65533/tcp open     unknown
65534/tcp open     unknown
65535/tcp open     unknown

# Nmap done at Fri Oct  2 12:33:50 2015 -- 1 IP address (1 host up) scanned in 2442.49 seconds
```

Şekil 5.12 Portspoof aracı açıkken yapılan tarama sonucu.

Açık portları tespit etmeye yönelik yapılan tarama sonuçları karşılaştırıldığında iki sonuca ulaşılabilir. Birincisi taramanın iki durumda ne kadar sürdüğü ve Portspoof aracının taramayı ne kadar yavaşlattığı. İkinci sonuç ise Portspoof sayesinde açık görünen portların saldırganlar için iyi bir sonuç olmaması. Çünkü tarama sonucunda elde edilen açık port sayısının çok olması saldırganların kafasını karıştırabilir ve tarama sonucuna şüpheli yaklaşmalarına neden olabilir.

Portspoof aracının yavaşlatmaya yönelik etkisini ölçmek için yapılan ikinci tarama testinin sonuçları, Portspoof kapalıyken ve Portspoof açıkken olmak üzere sırasıyla Şekil 5.13 ve Şekil 5.14'te verilmiştir.

```
# Nmap 6.47 scan initiated Fri Oct 16 11:55:16 2015 as: nmap -sS -sV -n -Pn -p1-1000 -oN tarama2_1 149.202.232.129
Nmap scan report for 149.202.232.129
Host is up (0.055s latency).
Not shown: 997 closed ports
PORT    STATE    SERVICE      VERSION
80/tcp  open     http         Apache httpd 2.4.10 ((Debian))
111/tcp open     rpcbind      2-4 (RPC #100000)
445/tcp filtered microsoft-ds

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
# Nmap done at Fri Oct 16 11:55:30 2015 -- 1 IP address (1 host up) scanned in 14.50 seconds
```

Şekil 5.13 Portspoof aracı kapalıyken yapılan taramanın sonucu.

```
# Nmap 6.47 scan initiated Fri Oct 16 11:38:08 2015 as: nmap -sS -sV -n -Pn -p1-1000 -oN tarama2_2 149.202.232.129
Warning: Servicescan failed to fill product_template (subjectlen: 46, productlen: 80). Capture exceeds length? Match string was lin
e 8048: p/ADB P.DG A4001N WAP, Cisco Telepresence MCU 4505, or Digifort Enterprise 6.5 httpd//
Nmap scan report for 149.202.232.129
Host is up (0.057s latency).
PORT     STATE    SERVICE          VERSION
1/tcp    open     pop3             Microsoft Exchange 2003 pop3d 6 (Taiwanese)
2/tcp    open     compressnet?
3/tcp    open     compressnet?
4/tcp    open     unknown
5/tcp    open     unknown
6/tcp    open     telnet           Eaton Powerware Environmental Rack Monitor telnetd
7/tcp    open     http             WYM httpd U-RXcg (A+V Link NVS-4000 surveillance system http config)
8/tcp    open     http             IP_SHARER WEB Pm (TRENDnet router http config; being managed by 936)
9/tcp    open     http             Dbox2 Neutrino httpd
10/tcp   open     ssh              Xlight FTP Server sshd FN (protocol 4)
11/tcp   open     http             McAfee ePolicy Orchestrator http interface
12/tcp   open     unknown
13/tcp   open     ssh              DrayTek Vigor 2820n ADSL router sshd r (protocol 939)
14/tcp   open     irc              IRC2000 Pro ircd
15/tcp   open     netstat?
16/tcp   open     unknown
17/tcp   open     telnet           Nortel Baystack 470-48t switch telnetd
  ...      ...       ...
994/tcp  open     http             eHTTP IqJAdZKV (HP ZRJaIzjf http config)
995/tcp  open     pop3s?
996/tcp  open     telnet           Carrier Access Adit 600 telnetd
997/tcp  open     biff             NotifyMail biffd
998/tcp  open     busboy?
999/tcp  open     http             NetPort httpd 4190 (NEC Projector http config)
1000/tcp open     cadlock?
Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
# Nmap done at Fri Oct 16 11:48:59 2015 -- 1 IP address (1 host up) scanned in 651.62 seconds
```

Şekil 5.14 Portspoof aracı açıkken yapılan tarama sonucu.

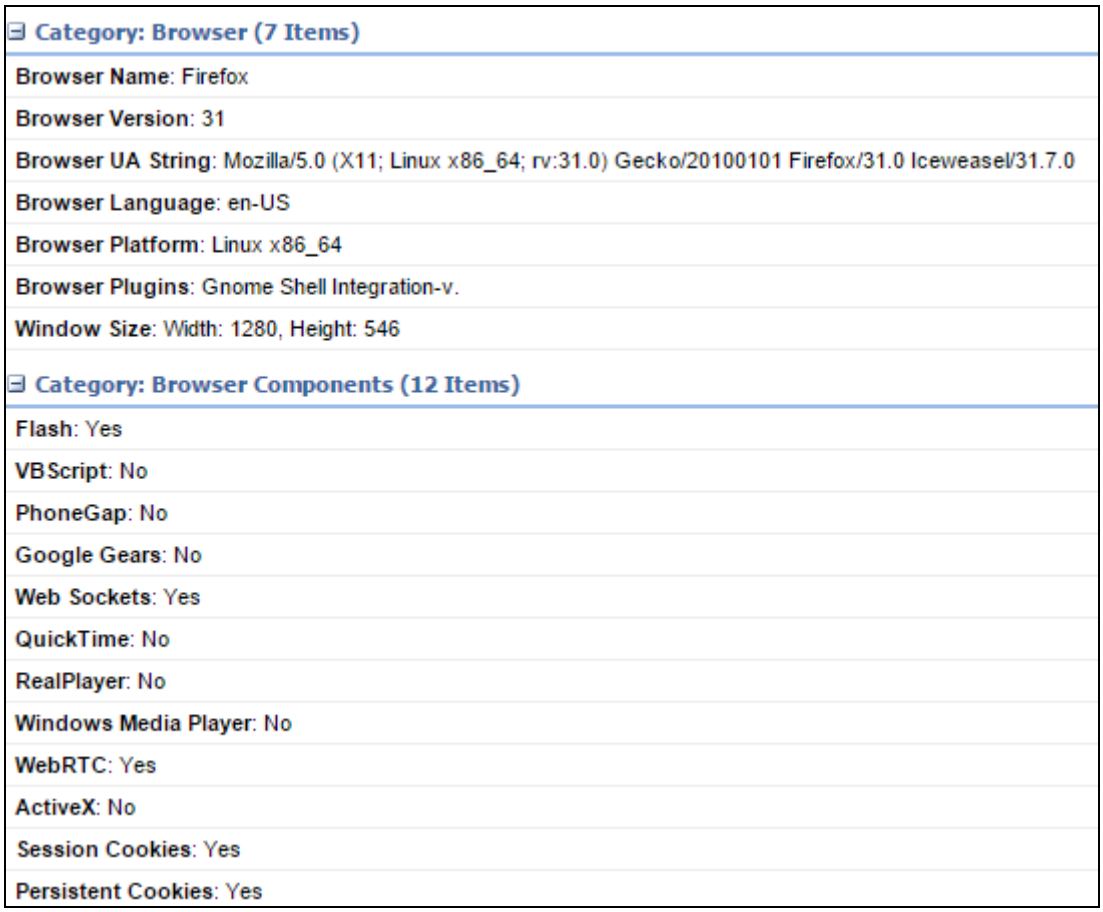
İkinci aşamada yapılan taramalarda da Portspoof aracının etkisinin birinci tarama ile benzer olduğu söylenebilir. Ancak birinci taramaya ilaveten, bu taramada portlarda çalışan servislerin tespit edilmeye çalışılması ve Portspoof aracının portlar üzerinde servis çalışıyor gibi sonuç alınmasını sağlaması saldırganlar açısından daha karmaşık bir durum olabilir. Çünkü ilk tarama sonucunda portlar üzerinde aynı servis çalışıyormuş gibi bir sonuç alınması, saldırganların bu durumu yanlış pozitif (false positive) olarak değerlendirmesine sebep olabilir. Fakat ikinci tarama sonucunda elde edilen verilerde her port üzerinde özgün (unique) bir servis çalışıyor gibi görünmesi daha inandırıcı olacaktır.

Portspoof aracı ile ağ keşif çalışmalarını yavaşlatmaya yönelik yapılan testlerde, sonucun olumlu olduğu ve bu araç sayesinde Nmap ile yapılan taramaların daha uzun sürede tamamlandığı tespit edilmiştir. Buna ilaveten aracın tarama sonuçlarına olumlu yanıt dönmesinin yanında portlar üzerinde bir servis çalışıyor gibi cevap dönmesi de aldatmaya yönelik etkili bir araç olarak da kullanılabileceğini göstermektedir. Yani saldırıyı yavaşlatmak ve saldırganı aldatmak adına başarılı bir araç olarak kullanılabileceği savunulabilir. Ancak Portspoof aracının etkisini ölçmeye yönelik yapılan testler daha iyi imkânlar çerçevesinde daha etkili yapılabilirdi. Bu deneyde sadece ağ tarama aracının ne kadar süre yavaşlatılabildiği ölçülmüştür. Ayrıca aktif siber savunma kapsamında ölçülmesi hedeflenen yavaşlatma etkisi sadece ağ tarama aracının yavaşlamasını ölçmek olmamalıdır. Önemli olan nokta saldırganın ağ yapısını tespit etmesi ve topolojiyi çıkartırken yavaşlatılmasındaki etkiyi ölçebilmektir. Buna ilaveten yapılan bu deneyde aldatma etkisini ölçmek mümkün değildir. Eğer laboratuvar daha geniş bir ağ topolojisi ile kurulabilseydi ve saldırgandan bu ağ topolojisinin çıkartılması istenseydi aldatma etkisi ve saldırganın ne kadar yavaşlatıldığı ve yakalanma ihtimali daha iyi ölçülebilirdi.

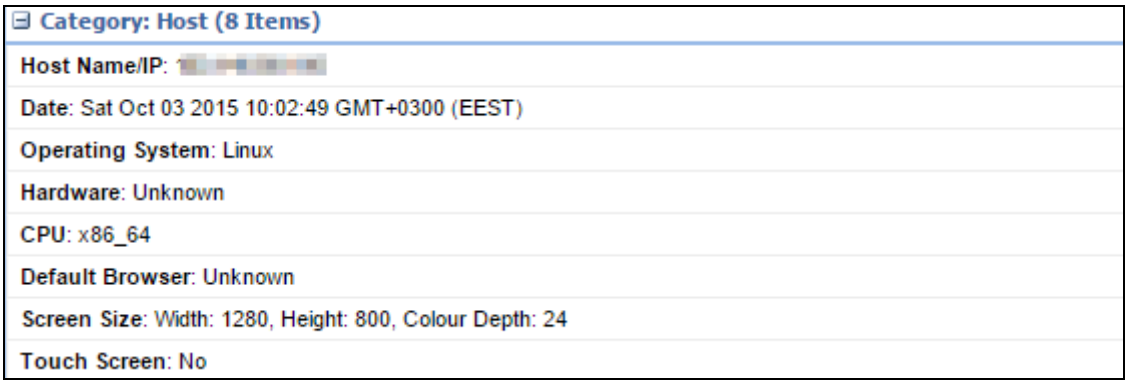
5.4 Karşı Atak Testi Sonucu

Saldırganın balküpü üzerindeki sayfayı ziyaret etmesinden sonra beklendiği üzere tarayıcısı ele geçirilmiştir ve BeEF aracının kontrol paneline bağlantı bilgisi gelmiştir. Saldırganın sayfayı ziyaret etmesi ve tarayıcının ele geçirilmesi sonucu tarayıcısı hakkında elde edilen bilgiler Şekil 5.15 ve saldırganın makinesi hakkında elde edilen

bilgiler Şekil 5.16'da gösterilmiştir.



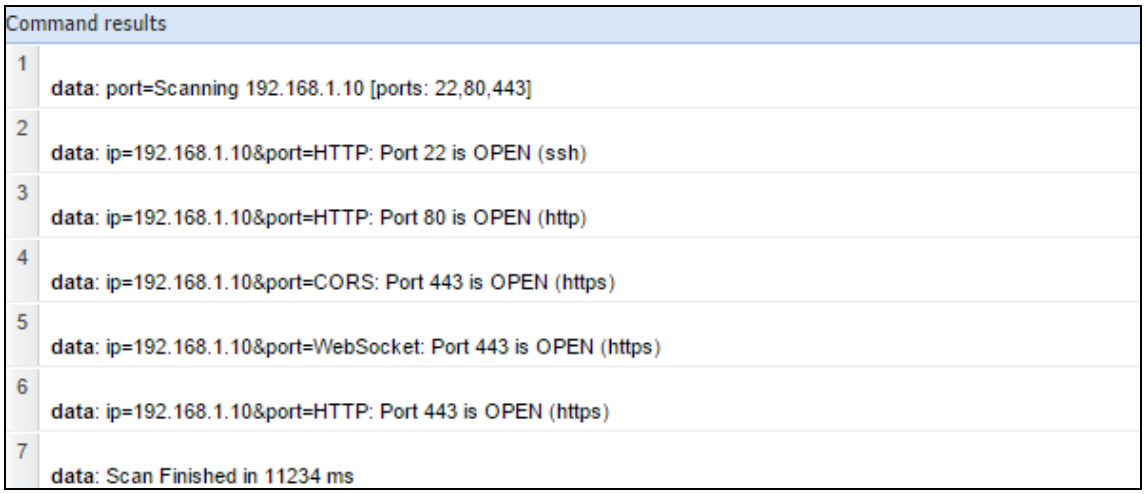
Şekil 5.15 Saldırganın tarayıcısı hakkında bilgiler.



Şekil 5.16 Saldırganın makinesi hakkında bilgiler.

BeEF üzerinde bulunan modüller kullanılarak ele geçirilen saldırgan makineye veya ağına yönelik saldırılar yapılabilir. Laboratuvar çalışmalarında örnek olarak 'Port Scanner' modülü ile saldırganın makinesine yönelik port taraması yapılmıştır. Şekil

5.17'de saldırgan makinenin 22, 80 ve 443. Portuna yönelik yapılan tarama sonucu gösterilmiştir.



Şekil 5.17 Saldırgan makineye yönelik port taraması.

Karşı atak testleri kapsamında BeEF aracı ile yapılan testlerin sonucunun da başarılı olduğu gözlemlenmiştir. Zararlı sayfayı ziyaret eden saldırganın tarayıcısının ele geçirildiği gözlemlenmiştir. Buna ilaveten, BeEF aracı üzerindeki modüller kullanılarak, ele geçirilen tarayıcı üzerinden saldırgana yönelik ataklar bir adım daha ilerletilmiştir. Bu sayede saldırgan makinesi üzerinden taramalar yaparak saldırgan hakkında daha detaylı bilgi toplanabildiği tespit edilmiştir. BeEF aracı üzerindeki modüller incelediğinde karşı atak kapsamında daha farklı ataklar yapılabileceği de savunulabilir. Bunlara karşın BeEF aracının karşı ataklar için kullanışlı bir araç olmasının yanında eksik kalan yönlerinin olduğu savunulabilir. Saldırgan makinesi ele geçirildiğinde eğer kalıcılık (persistence) sağlanamaz ise saldırgan elden kaçırılabilir. Diğer bir eksik nokta ise, BeEF tarayıcıları sömürmeye yönelik bir araç olduğu için, saldırganın ele geçirilmesi ve diğer saldırıların başarılı olması, tarayıcı ayarlarına göre değişiklik göstermektedir.

6. TARTIŞMA

Bu tez çalışması kapsamında yapılan literatür taramaları ve laboratuvar çalışmalarının sonucunda aktif siber savunmanın geleneksel savunma sistemleri yerine yeni bir alternatif değil aksine geleneksel savunma sistemlerine ilave bir güvenlik mekanizması olarak kullanılması gerektiği tespit edilmiştir. Güvenlik duvarı, IPS/IDS vb. geleneksel güvenlik çözümü olarak adlandırılan mekanizmalar güvenlik sisteminin olmazsa olmazları arasında yer aldığı görülmüştür.

Aktif siber savunma tekniklerinin, güvenliği artırmaya çalışırken aynı zamanda saldırganları yavaşlatmayı ve saldırıların etkisini azaltmayı amaçladığı da görülmüştür. Ayrıca saldırganları durdurmak hatta yok etmek gibi daha agresif çözümlerinde aktif siber savunma yaklaşımı çerçevesinde ele alındığı görülmüştür.

Kamu kurumlarında güvenliği artırmak adına aktif siber savunma yaklaşımının nasıl kullanılabileceği bu tez çalışmasının ana hedefleri arasında yer almıştı. Aktif siber savunmanın etkisini ölçmek amacıyla kurulan laboratuvar ortamı birkaç tane sanal makine ve basit web uygulamaları ile kurulmuştu. Buna rağmen aktif siber savunma tekniklerinin siber saldırılar karşısında etkili olabileceği kısmen de olsa gözlemlenmiştir. Ancak kamu kurumlarının ağları genel olarak değerlendirildiğinde, hizmet verdikleri kitle, kurum çalışan sayıları, web uygulamaları gibi ağ yapısını etkileyen bileşenler göz önüne alındığında ağlarının çok daha büyük olduğunu tahmin etmek zor olmayacaktır. Bu kurumların ağ yapısının büyüklüğü ve karmaşıklığı göz önüne alındığında aktif siber savunma yöntemlerinin güvenliği artırmaya katkısının daha büyük olacağı savunulabilecektir. Örnek vermek gerekirse, laboratuvar ortamında Portspoof aracıyla yapılan deneyde sadece ağ taramasını yavaşlatmaya yönelik etkisi kısmen gözlemlenebilmişti. Kamu kurumlarındaki ağ cihazlarının, sunucuların ve güvenlik ürünleri gibi birçok ürünün veya uygulamanın yönetimi, veri aktarımı vb. yönetimsel ihtiyaçlar için ssh, telnet vb. servislerin kullanıldığı bilgisayar korsanları, güvenlik uzmanları hatta kurumlarda çalışan çoğu çalışan tarafından bilinmektedir. Saldırganlar sistemlere sızmak için ilk önce keşif çalışması yaparlar. Bu yönetimsel servislerin açık kapalı olma durumunu tespit etmeye çalışırlar. Saldırganların bu çalışmasını boşa çıkartmak en azından yavaşlatma amacıyla Portspoof aracı

kullanılabilir. Saldırganlar ilk olarak bu servisleri doğal olarak varsayılan portlar üzerinde arayacaklar. Bazı kurum çalışanları güvenlik amacı ile bu servisleri varsayılan portları dışında bir portta çalıştırarak kısmen önlem almış olsa da saldırganların bu portları tespit etmesinin önüne geçemezler. Ancak varsayılan portu kapatmak yerine Portspoof aracına yönlendirirse ve saldırganların keşif taramalarında port kapalı yerine servis çalışıyor gibi cevap almaları sağlanarak yanıltılması daha etkili bir savunma olacaktır. Saldırganlar içinde bulundukları durumu anlamaya çalışırken daha fazla tarama ihtiyacı hissedecekler. Bu durum saldırganların motivasyonunu düşürürken daha fazla zaman harcamalarına neden olacaktır. Ayrıca fazladan yapılan her tarama yakalanma ihtimalini de artıracaktır. Bunlara ilaveten Portspoof aracının sunucu kaynaklarını fazla tüketmeyen Python tabanlı bir uygulama olduğu göz önüne alınırsa ve geleneksel güvenlik ürünleri için harcanan büyük miktarlar karşısında ücretsiz bir uygulama olduğu dikkate alınırsa güvenliği artırmak adına kurumlardaki tüm sunucu ve bilgisayarlarda çalıştırılmasının büyük bir maliyet oluşturmayacağı savunulabilir. Hatta güvenliği artırma adına etkisinin de büyük olacağı iddia edilebilir. Saldırganın büyük bir ağda yaptığı tüm keşif çalışmalarının pozitif yanlış (false pozitive) olduğunu görmek canını sıkacak ve motivasyonunu düşürecektir.

Karşı atak teknikleri kamu kurumlarında nasıl kullanılabilir sorusuna cevap olarak en basit şekliyle laboratuvar ortamındaki gibi bir balküpü kurulabilir. Kamu kurumlarının çoğunda birden fazla web uygulaması vardır. Ayrıca kamu kurumlarında farklı nedenlerden dolayı üretim ortamı, test ortamı, eğitim ortamı ve gerçek ortam gibi yaklaşımlar kullanılır. Gerçek ortamdaki web uygulamaları kurumun kamuya hizmet verdiği, kamu tarafından bilinen ve genellikle de DNS adı kullanılarak erişilen uygulamalardır. Ancak saldırganlar pasif keşif aşamalarında ne kadar DNS adı kullansalar da aktif keşif aşamasına geçtiklerinde IP adreslerini kullanırlar ve kurumların internete açık diğer sunucularını tespit etmeye çalışırlar. İnandırıcılık açısından iyi hazırlanmış bir balküpü internet ortamına bir nevi test uygulaması gibi açılırsa saldırganların bu uygulamayı ziyaret etmeleri sağlanabilir. Bu şekilde saldırganlar hakkında daha fazla bilgi toplanabilir hatta saldırgan makineleri ele geçirilebilir.

Aktif siber savunma kapsamında yavaşlatma etkisini ölçmek amacıyla laboratuvar ortamında incelenen bir diğer uygulama ise Spidertrap uygulamasıydı. Bu uygulama kamu kurumlarında birden fazla farklı amaç için kullanılabilir. DMZ bölgesindeki bir balküpü olan bir web uygulaması üzerine yapılandırma ayarları eksik yapılmış bir test sunucusu görünümü verilebilir ve bu uygulama üzerinde hazırlanan anahtar kelimeler dizin şeklinde görülür. Normal kullanıcıların DNS adı ile erişemeyeceği bu sunucuyu saldırganlar, dış ağ IP'lerini tespit ettiklerinde erişim sağlayabilirler. Böylece hazırlanan anahtar dizinleri ziyaret ettiklerinde saldırganların ne aradığı hakkında bilgi elde edilebilir. Ayrıca otomatik tarama aracı ile de tarama yaparlar ise taramalarının yavaşlamasına neden olacaktır.

Yapılan çalışmalar ve aktif siber savunma yöntemleri ve yaklaşımları ele alındığında, aktif siber savunmanın dinamik bir çözüm olduğu görülmektedir. Bunun yanında aktif siber savunmanın stratejik bir yaklaşım olduğu da savunulabilir. Saldırı potansiyellerini tespit edip bunlara yönelik dinamik önlemler alınması da aktif siber savunma kapsamında değerlendirilebilir.

7. KAYNAKLAR

Alperovitch, D. (2011). Revealed: Operation Shady Rat. McAfee.

Anderson, R., Lum, B., & Walha, B. (2005, December 11). Offense Vs Defense. Washington: University of Washington.

Dittrich, D., & Himma, K. E. (2005). ACTIVE RESPONSE TO COMPUTER INTRUSIONS. Hoboken, N.J.: John Wiley & Sons, Inc.

Even, L. R. (2000, July 12). Intrusion Detection FAQ: What is a Honeypot? Swansea, UK: SANS Institute.

Gökırmak, Y., Yüce, E., Bektaş, O., Soysal, M., & Orcan, S. (2009). IPv6 Balküpü Tasarımı. EMO Elektrik-Elektronik, Bilgisayar ve Biyomedikal Mühendisliği Ulusal Kongresi, Aralık.

Grudziecki, T., Jacewicz, P., Juszczyk, Ł., Kijewski, P., & Pawliński, P. (2012, Kasım 10). Proactive Detection of Security Incidents. ENISA.

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Leading Issues in Information Warfare & Security Research.

Isoda, Y. (2014, October 3). Use Japanese Castles to Better Communicate Defense-in-Depth Strategies. Gartner.

Johnson, J., & Northcutt, S. (2013). Implementing Active Defense Systems on Private Networks. SANS Institute.

Kara, M. (2013). Siber Saldirilar - Siber Savaşlar Ve Etkileri. Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi.

Karaarslan, E., Akın, G., & Fetah, V. (2008, 04 16). Kurumsal Ağlarda Zararlı Yazılımlarla Mücadele Kılavuzu . ULAK-CSIRT, TÜBİTAK - ULAKBİM .

Lachow, I. (2013, February). Active Cyber Defense A Framework for Policymakers. Center for a New American Security.

Lu, W., Xu, S., & Yi, X. (2013, November 11). Optimizing Active Cyber Defense. Decision and Game Theory for Security. Fort Worth, Texas, USA: 4th International Conference, GameSe.

McGee, S., Sabett, R. V., & Shah, A. (2013). Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense. 8 J. Bus. & Tech. L. 1.

Mitnick, K. D., Simon, L. W., & Wozniak, S. (2003). The Art of Deception: Controlling the Human Element of Security. New York: Wiley Publishing.

Orans, L., & D'Hoinne, J. (2013, August 20). Five Styles of Advanced Threat Defense. Gartner.

Öğün, M. N., & Kaya, A. (2013). Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler. Güvenlik Stratejileri Yıl:9 Sayı:18.

Pingree, L., MacDonald, N., & Firstbrook, P. (2013, September 12). Best Practices for Mitigating Advanced Persistent Threats. Gartner.

Repik, K. A. (2008, June). Defeating Adversary Network Intelligence Efforts with Active Cyber Defense Techniques. Ohio, USA: THE AIR FORCE AIR UNIVERSITY.

ResmiGazete. (2013, 06 20). Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı. Ankara: Resmi Gazete.

Rouse, M. (2006, October 23). Definition Social Engineering. www.techtarget.com.

Soysal, M., Bektaş, O., & Üçtop, K. (2015, Eylül 30). Ulak CSIRT Balküpü Tuzağı ve Kara Delik Çalışma Grubu.

Vaarandi, R. (2013). Detecting Anomalous Network Traffic in Organizational Private Networks. Proceedings of the 2013 IEEE International Multi-Disciplinary Conference on.

Vural, Y., Bayındır, M., & Tamer, O. (2009, Şubat 11). Anayurt Güvenliğinin Sağlanmasında Bilgi Sistemleri Güvenliğinin Önemi. Şanlıurfa: Akademik Bilişim Konferansı Bildirileri 11-13 Şubat 2009 Harran Üniversitesi.

Zhuang, R., Zhang, S., DeLoach, S. A., Ou, X., & Singhal, A. (2012, June). Simulation-based Approaches to Studying Effectiveness of Moving-Target Network Defense . National Symposium on Moving Target Research. 2012.

İnternet Kaynakları

1. Anonim, (2012). Active Defense Strategy for Cyber. MITRE. http://www.mitre.org/publications/technical-papers/active-defense-strategy-for-cyber.
2. Anonim, (2014). Deloitte Global Siber Güvenlik Yönetici Bilgilendirme Raporu.

Deloitte. http://www2.deloitte.com/tr/tr/pages/risk/articles/Global-Cyber-Briefing.html.

3. Anonim, (2015). APT30 AND THE MECHANICS OF A LONG-RUNNING CYBER ESPIONAGE OPERATION. FireEye. https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf.

4. Anonim, (2013). APT1. Exposing One of China's Cyber Espionage Units. Mandiant. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

5. Anonim, (2015). Internet Security Threat Report 20. Symantec. http://www.symantec.com/security_response/publications/threatreport.jsp.

6. Altundal, Ö. F. (2014). Siber Güvenlik Raporu 2014. http://www.siberguvenlik.org.tr/2015/01/2014-Siber-Guvenlik-Raporu-Yayinlandi.html.

7. Al Jazeera. (2014). Sony DDOS Saldırılarına Başladı. http://www.aljazeera.com.tr/haber/sony-ddos-saldirilarina-basladi.

8. Caniklioğlu, E. (2013). Rusya ve Türkiye: Casusluk Vakalarının Değişen Niteliği. http://www.21yyte.org/arastirma/milli-guvenlik-ve-dis-politika-arastirmalari-merkezi/2013/08/10/7149/rusya-ve-turkiye-casusluk-vakalarinin-degisen-niteligi.

9. Çelik, M. (2015). Şirketler Siber Silahlara Sarılırsa. http://siberbulten.com/makale-analiz/sirketler-siber-silahlara-sarilirsa/.

10. Çevik, F. (2014). Redhack Türk Hukukunun Neresinde? http://siberbulten.com/makale-analiz/redhack-turk-hukukunun-neresinde/.

11. Duszynski, P. (2013). Fun with 'Active Defense'. www.trustwave.com: https://www.trustwave.com/Resources/SpiderLabs-Blog/Fun-with--Active-Defense-/#more

12. Hosenball, M., & Spetalnick, M. (2015). U.S. urged to tighten cyber security to counter Chinese hacking. Washington: http://www.reuters.com/article/us-usa-cybersecurity-idUSKCN0RA28M20150910.

13. Security, B. H. (2015). Active Defense Harbinger Distribution. http://www.blackhillsinfosec.com/#!projects/cfam.

14. Siber Bülten. (2015,a). Çin Yeni Askeri Stratejisini Açıkladı: Stratejide Savunma, Operasyonda Saldırı. 13. http://siberbulten.com/uncategorized/cin-

yeni-askeri-stratejisini-acikladi-stratejide-savunma-operasyonda-saldiri/.

15. Siber Bülten. (2015,b). Washington, Siber Saldırılara Karşı Yaptırım Uygulayacak. http://siberbulten.com/uluslararasi-iliskiler/abd/washington-siber-saldirilara-karsi-yaptirim-uygulayacak/.

16. Symantec. (2015). What is a Zero-Day Vulnerability? http://www.pctools.com/security-news/zero-day-vulnerability/.

17. Toivola, T. (2002). vnStat. http://humdi.net/vnstat/.

18. Yener, Y. (2015). Bir Bilim-Kurgu Romanından Fazlası: Guguk Kuşu Yumurtası. www.siberbülten.com.

ÖZGEÇMİŞ

Adı Soyadı : Recep ÖZBAY

Doğum Yeri ve Tarihi : 28.03.1989

Yabancı Dili : İngilizce

İletişim (Telefon/e-posta) : 0541 436 4306 / ozbayrecep@gmail.com

Eğitim Durumu (Kurum ve Yıl)

Lise : Konuralp Anadolu Lisesi - 2007

Lisans : Anadolu Üniversitesi - 2012

Yüksek Lisans : Afyon Kocatepe Üniversitesi 2014-2016

Çalıştığı Kurum/Kurumlar ve Yıl :TÜBİTAK BİLGEM SGE - 2012 / Devam Ediyor