T.C.

TRAKYA ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

TÜRKİYE VE DÜNYADA GERÇEKLEŞTİRİLEN SİBER SALDIRI YÖNTEMLERİNİN VE BU SALDIRILARA KARŞI ALINAN ÖNLEMLERİN İNCELENMESİ

SÜMEYRA TEK

YÜKSEK LİSANS TEZİ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

Tez Danışmanı: Dr. Öğr. Üyesi ANDAÇ ŞAHİN MESUT

EDİRNE - 2022

Sümeyra TEK'in hazırladığı "**Türkiye ve Dünyada Gerçekleştirilen Siber Saldırıları Yöntemlerinin ve Bu Saldırılara Karşı Alınan Önlemlerin İncelenmesi**" başlıklı bu tez, tarafımızca okunmuş, kapsam ve niteliği açısından Bilgisayar Mühendisliği Anabilim Dalında bir **Yüksek Lisans tezi** olarak kabul edilmiştir.

Jüri Üyeleri:	İmza
Prof. Dr. M. Tolga SAKALLI	……
Dr. Öğr. Üyesi Andaç MESUT (Danışman)	……
Dr. Öğr. Üyesi H. Nusret BULUŞ	……

Tez Savunma Tarihi: 09/12/2022

Bu tezin Yüksek Lisans tezi olarak gerekli şartları sağladığını onaylarım.

İmza

Dr. Öğr. Üyesi Andaç MESUT
Tez Danışmanı ……

Trakya Üniversitesi Fen Bilimleri Enstitüsü onayı

……

Prof. Dr. Hüseyin Rıza Ferhat KARABULUT
Fen Bilimleri Enstitüsü Müdürü

T.Ü.FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ YÜKSEK LİSANS PROGRAMI
DOĞRULUK BEYANI

Trakya Üniversitesi Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında, tüm verilerin bilimsel ve akademik kurallar çerçevesinde elde edildiğini, kullanılan verilerde tahrifat yapılmadığını, tezin akademik ve etik kurallara uygun olarak yazıldığını, kullanılan tüm literatür bilgilerinin bilimsel normlara uygun bir şekilde kaynak gösterilerek ilgili tezde yer aldığını ve bu tezin tamamı ya da herhangi bir bölümünün daha önceden Trakya Üniversitesi ya da farklı bir üniversitede tez çalışması olarak sunulmadığını beyan ederim.

09 / 12 / 2022
Sümeyra TEK
İmza

Yüksek Lisans Tezi

Türkiye ve Dünyada Gerçekleştirilen Siber Saldırıları Yöntemlerinin ve Bu Saldırılara Karşı Alınan Önlemlerin İncelenmesi

T.Ü. Fen Bilimleri Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı

ÖZET

Ülkelerin dijital dönüşüm süreçlerinde, bilgi güvenliği en önemli konulardan biridir. Bu açıdan bireyler, toplum ve devletler açısından siber güvenlik sistemleri hem verilerin korunmasında hem de siber saldırılardan kaynaklı zararların önlenmesinde siber güvenlik önemli bir yere sahiptir. Günden güne artan dijitalleşme süreci, siber saldırı tehditlerinin ve internet üzerinde siber saldırılara karşı güvenlik açıklarının da aynı oranda artmasına neden olmaktadır. Kişisel verilerin ve devletlerin gizli bilgilerinin herhangi bir tehdide karşı korunması oluşabilecek ciddi maliyetler ve zararlardan koruyacaktır. Bu bağlamda siber güvenlik kavramı tezin temelini oluşturmaktadır. Bu açıdan siber güvenliğinin sağlanması için öncelikle tez çalışmasında siber saldırı türleri ve saldırılardan korunma yöntemleri incelenmektedir. Bunun yanında Türkiye'de ve Dünya üzerindeki siber saldırı örnekleri yöntemleri ile incelenecektir. Böylece hem literatür hem de alan uzmanlarına katkı sağlanması hedeflenmektedir. Son olarak siber güvenlik açısından farkındalığın da arttırılması tezin temel amaçlarından birini oluşturmaktadır.

Yıl : 2022

Sayfa Sayısı : 92

Anahtar Kelimeler : Siber Savaş, Siber Güvenlik, Siber Saldırı, Korunma Yöntemleri

Master's Degree Thesis

Examining the Methods of Cyber Attacks and the Measures Against These Attacks in Turkey and in the World

Trakya University Institute of Natural and Applied Sciences

Computer Engineer Department

ABSTRACT

In the digital transformation processes of countries, information security is one of the most important issues. In this respect, cyber security systems have an important place in both the protection of data and the prevention of damages caused by cyber attacks in terms of individuals, society and states. The increasing digitalization process day by day causes cyber threats and cyber security vulnerabilities to increase at the same rate. Protection of personal data and confidential information of governments against any threat will protect it from serious costs and damages that may occur. In this context, the concept of cyber security forms the basis of the thesis. In this respect, in order to ensure cyber security, first of all, types of cyber attacks and methods of protection from attacks are examined in the thesis. In addition, cyber security approaches and policies in Turkey and around the world will be examined. Thus, it is aimed to contribute to both the literature and the field experts. Finally, raising awareness in terms of cyber security is one of the main objectives of the thesis.

Year : 2022

Number of Pages : 92

Keywords : Cyber Warfare, Cyber Security, Cyber Attack, Protection Methods

TEŞEKKÜR

Bu çalışmanın tüm aşamalarında her zaman yanımda olup desteğini, bilgisini ve değerli görüşlerini hiçbir zaman esirgemeyen danışmanım Dr. Öğr. Üyesi Andaç ŞAHİN MESUT'a teşekkürlerimi bir borç bilirim.

Ayrıca tez aşaması sürecinde desteğini maddi manevi veren, zorlu ve stresli araştırma ve tez yazım sürecinde her zaman benim yanımda olan ve desteklerini hiçbir zaman esirgemeyen canım aileme sonsuz teşekkür ederim.

İÇİNDEKİLER

ÖZET iv
ABSTRACT v
TEŞEKKÜR vi
İÇİNDEKİLER vii
ŞEKİLLER DİZİNİ xi
ÇİZGELER DİZİNİ xii
SİMGELER VE KISALTMALAR DİZİNİ xiii
BÖLÜM 1 1
GİRİŞ 1
BÖLÜM 2 4
SİBER GÜVENLİK 4
2.1. Siber Güvenlik ve Savunmanın Önemi 8
2.2. Siber Güvenlik Kavramı ve İlişkili Tanımlar 8
2.3. Siber Kavramı 9
2.4. Siber Alan 10
2.5. Siber Uzay 11
2.6. Siber Suçlar 13
2.7. Siber Riskler ve Tehditler 13
2.8. Siber Terörizm 14
2.9. Kritik Altyapı 15
BÖLÜM 3 16
SİBER SALDIRILARI TÜRLERİ 16
3.1. Kötü Amaçlı Yazılımlar (Malware Software) 16
3.1.1 Fidye Yazılımı Saldırıları (Ransomware) 17
3.1.2. Solucanlar ve Kurtçuklar (Worms) 18
3.1.3. Bilgisayar Virüsleri 19
3.1.4. Truva Atı (Trojen) 19
3.1.5. Arka Kapı (Backdoor) 20
3.1.6. Casus Yazılımlar (Spyware) 20
3.1.7. Reklam Yazılımları (Adware) 21
3.1.8. Mantık Bombaları (Logic Bombs) 21

3.1.9. Bukalemun (Chamelon) 21
3.1.10. Kök Kullanıcı Takımı (Rootkit) 22
3.1.11. Mesaj Sağanağı (Spam,Junkmail) 22
3.1.12. Tarayıcı Ele Geçirme-Soyma (Browser Hijacking) 22
3.1.13. Korunmasızlık Sömürücü (Exploit) 23
3.1.14. Klavye Dinleme Sistemi (Keylogger) 23
3.1.15. Telefon Çevirici (Dialer) 23
3.1.16. Ekran Kaydedici Yazılımlar (Screenlogger) 24
3.2. Kimlik Avı - Oltalama Saldırıları (Phishing) 24
3.3. Ortadaki Adam Saldırısı (Man in the Middle -MITM) 25
3.4. Servis Reddi Saldırıları (DoS-Denial of Service, DDoS-Distributed Denial of Service) 25
3.5. Kimlik Bilgisi Doldurma Saldırıları (Credential Stuffing Saldırıları) 26
3.6. Şifre Saldırıları (Password Attack) 27
3.6.1. Kaba Kuvvet Saldırısı (Brute Force Attack) 28
3.6.2. Sözcük Tabanlı Saldırılar (Dictionary-Based Attack) 28
3.7. ARP Spoofing 28
3.8. DNS Spoofing 29
3.9. DHCP Starvation 30
3.10. DHCP Spoofing 31
3.11. Sosyal Mühendislik Saldırıları 32
BÖLÜM 4 33
SİBER SALDIRILARDAN KORUNMA YÖNTEMLERİ 33
4.1. Şifreleme 33
4.2. Sayısal İmza 34
4.3. Steganografi 36
4.4. Kimlik Doğrulama 36
4.5. Firewall (Ağ Güvenlik Duvarı) 37
4.6. Saldırı Tespit ve Engelleme Sistemleri (IDS/IPS) 39
4.7. Antivirüs 40
BÖLÜM 5 42
SİBER SALDIRI ÖRNEKLERİ 42
5.1. Dünya Genelinde Siber Saldırı Örnekleri 42

5.1.1. Sibirya Siber Saldırısı (Logic Bomb) 42
5.1.2. Ay Işığı Labirenti (Moonlight Moze) 43
5.1.3. Melisa 43
5.1.4. NATO Siber Saldırısı 43
5.1.5. World of Hell 44
5.1.6. Estonya Siber Saldırısı 44
5.1.7. Black Energy 44
5.1.8. DarkHotel 45
5.1.9. Litvanya Siber Saldırısı 45
5.1.10. Gürcistan Siber Saldırısı 45
5.1.11. Rocra APT Saldırısı 45
5.1.12. Güney Kore Siber Saldırıları 46
5.1.13. GhostNet 46
5.1.14. Stuxnet 46
5.1.15. GoDaddy Saldırısı 47
5.1.16. CryptoLocker 47
5.1.17. Kill Disk 47
5.1.18. Ukrayna Siber Saldırısı 47
5.1.19. Mirai 48
5.1.20. Atlanta Siber Saldırısı 48
5.1.21. NotPetya / ExPetr 48
5.1.22. WannaCry 49
5.1.23. US Universities 50
5.1.24. Github 50
5.1.25. Rampant Veri Sızıntısı 51
5.1.26. Almanya Siber Saldırısı 51
5.1.27. İsrail Siber Saldırısı (Black Shadow) 51
5.1.28. İrlanda Siber Saldırısı 52
5.1.29. PseudoManuscrypt 52
5.1.30. Norveç Siber Saldırısı 52
5.2.Türkiye'den Siber Saldırı Örnekleri 56

5.2.1. Bakü-Ceyhan-Tiflis Boru Hattı Saldırısı 56
5.2.2. Conficker 56
5.2.3. Türkiye İletişim Başkanlığına (TİB) Yönelik Siber Saldırı 57
5.2.4. Sağlık Bakanlığına Yönelik Siber Saldırı 57
5.2.5. Muddy Water (APT) Siber İstihbarat Saldırısı 58
5.2.6. Türk Telekom'a Yönelik Siber Saldırı 58
5.2.7. Yemeksepetine Yönelik Siber Saldırı 59
5.2.8. Konya Büyükşehir Belediyesine Yönelik Siber Saldırı 59
5.2.9. Medlife Sağlık Kurumuna Yönelik Siber Saldırı 60
5.2.10. Pegasus Siber Saldırısı 61
5.2.11. ALtahrea Saldırısı 61
5.2.12. Baydöner Restorana Yönelik Siber Saldırı 61
5.2.13. Tübitak'a Yönelik Siber Saldırı 61
5.2.14. MurenShark 62
5.2.15. THY Saldırısı 62
BÖLÜM 6 65
SONUÇ VE TARTIŞMA 65
KAYNAKLAR 69
ÖZGEÇMİŞ 79

ŞEKİLLER DİZİNİ

Şekil 2.1. Maslow'un İhtiyaçlar Hiyerarşisi 4
Şekil 3.1. Ortadaki Adam Atağı Yapısı ……..……..... 25
Şekil 3.2. ARP Spoofing Saldırı Örneği 29
Şekil 3.3. DNS Spoofing Saldırı Örneği 30
Şekil 3.4. DHCP Starvation Saldırı Örneği 31
Şekil 3.5. DHCP Spoofing Saldırı Örneği 32
Şekil 4.1. Şifreleme Yöntemleri …….. 34
Şekil 4.2. Sayısal İmza ……... 35
Şekil 4.3. Kimlik Doğrulama ……..... 37
Şekil 4.4. Firewall …….. 39
Şekil 4.5. IDS/IPS …….. 40
Şekil 5.1. NotPetya Saldırısı ……... 49
Şekil 5.2. WannaCry Saldırısı ……. 50
Şekil 5.3. Confiker Saldırısı 57
Şekil 5.4. Muddy Water (APT) Saldırısı ……..... 58
Şekil 5.5. Türk Telekom'a Siber Saldırı ……. 59
Şekil 5.6. Saldırıda Çalınan Veriler ……..... 60
Şekil 5.7. MurenShark Saldırısı …….. 62
Şekil 6.1. Dünya'da Gerçekleşen Siber Saldırı Türü Oranları ……..... 66
Şekil 6.2. Dünya'da Kritik Altyapılara Yönelik Gerçekleşen Siber Saldırı Türü Oranı … 66
Şekil 6.3. Türkiye'de Gerçekleşen Siber Saldırı Türü Oranları …….…… 67
Şekil 6.4. Türkiye'de Kritik Altyapılara Yönelik Gerçekleşen Siber Saldırı Türü Oranı... 68

ÇİZGELER DİZİNİ

Çizge 3.1. Zayıf Şifre Örnekleri 27

Çizge 5.1. Dünya Üzerinde Yapılmış Siber Saldırı Örnek Listesi..... 53

Çizge 5.2. Türkiye'ye Yönelik Yapılmış Siber Saldırı Örnekleri Listesi 63

SİMGELER VE KISALTMALAR DİZİNİ

APT	Advanced Persistent Threat
ARP	Address Resolution Protocol
AGİT	Avrupa Güvenlik ve İşbirliği Teşkilatı
BIT	Bilgi ve İletişim Teknolojileri
CVE	Common Vulnerabilities and Exposures
DoS	Disk Operating System
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DOJ	Department of Justice
IDS	Intrusion Detection Systems
IPS	Intrusion Prevention Systems
IIS	Internet Information Services
IP	Internet Protocol
IOT	Internet of Things
KOBİ	Küçük ve Orta Büyüklükteki İşletmeler
LAN	Local Area Network
MAC	Media Access Control
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
PLC	Programmable Logic Controllers
SCADA	Supervisory Control and Data Acquisition
SOME	Siber Olaylara Müdahale Ekipleri
TCP	Transmission Control Protocol
UETA	Uzak Erişim Truva Atı

BÖLÜM 1

GİRİŞ

İnternetin ilk ortaya çıkışı 1960'lı yıllarda ABD Savunma Bakanlığı tarafından geliştirilen ARPANET projesi ile gerçekleşmiştir. Bu projenin amacı başta haberleşme, şifreleme ve şifre çözme olsa da zamanla diğer alanlarda da kullanılmaya başlanmıştır. Son kullanıcılar açısından 1990 yılı başlarında geliştirilen World Wide Web, dünya Çapında Ağ (kısaca WWW veya Web), internet üzerinden bilgi paylaşımı sağlayan bir yöntem olarak hayatımıza girmiştir. İnternet ve üzerindeki bilgi paylaşımının yaygınlaşması internet kullanıcı sayısını zaman içerisinde arttırmıştır. We are Social 2022 yılı dijitalleşme raporunda internet kullanıcı sayısının son 10 yıl içinde iki kat arttığı rapor edilmiştir. Rapora göre 2012'nin başında 2,18 milyar olan kullanıcı sayısı 2022'nin başında 4,95 milyara çıkmıştır (We are Social, 2022). Bu rakam dünya nüfusunun yaklaşık %62,5'lik kısmını oluşturmaktadır. Özellikle pandemi sürecinin de etkisi ile tüm dünyada dijitalleşme hızlı bir ivme kazanmıştır. Bu durumdan hareketle bilgisayar, mobil cihazlar ve internet kullanımı kamu, özel sektör ve bireysel boyutta hayatımızın vazgeçilmez bir parçası olduğu yadsınamaz bir gerçek haline gelmiştir. Ayrıca makine öğrenmesi ve IOT teknolojileri ile internetin bir nevi siber dünyanın nüfusu artmış ve siber alan genişlemiştir.

Bilgi ve iletişim teknolojilerinde (BIT) gerçekleşen hızlı gelişim ile hem bireyler hem de toplumlar etkilenmektedir. Özellikle bilgisayarlar ve mobil cihazlar kullanılarak oluşturulan mekanizmalar, gerçek dünyaya ek olarak "siber alan" lar ortaya çıkarmıştır. Bu alan sayesinde bireyler ve toplumlar günlük hayatlarında karşılaştıkları zorlukların üstesinden gelmektedir (Gürkaynak ve İren, 2011). Fakat siber alanın doğuşu ve günden güne genişlemesi hem kullanıcılar hem de devletler için pek çok güvenlik riskini beraberinde

getirmiştir (Bıçakcı, Ergun ve Çelikpala, 2015). Bu güvenlik risklerinin başında siber saldırılar gelmektedir.

Siber saldırı, bir veya birden fazla bilgisayar vasıtasıyla kurbanın bilgisayar sistemlerine veya ağlarına, verilere habersizce ulaşmak, oynamak ya da verileri ortadan kaldırmak için çeşitli yöntemler ve yollar aracılığıyla yapılan saldırı eylemlerinin tamamı olarak ifade edilmektedir (Karel, 2019). Siber saldırılar internetin yaygınlaşması ve teknolojinin her alana girmesiyle etkinliğini arttırmıştır. Özellikle görüldüğü gibi günümüzde teknolojik gelişmeler ile özel sektör ve kamu kuruluşlarının operasyonlarının birçoğu dijital ortama taşınmıştır. Böylelikle siber saldırıların sıklığı ve tehdit ettiği ortamlar hızla değişmektedir. Siber saldırıların artmasıyla kişiler, kurumlar ve ülkeler zarar görmektedir. Literatürde siber saldırıların verdiği zararların sınıflandırılması incelendiğinde "fiziksel veya dijital zarar", "ekonomik zarar", "psikolojik zarar", "itibar zararı", "sosyal ve toplumsal zarar" karşımıza çıkmaktadır (Agrafiotis vd., 2018). Görüldüğü gibi günden güne artan siber saldırıların zararları geniş bir alana yayılmaktadır. Bu durum değişen dünya değerleri ve teknolojik gelişmeler ile daha da tehlikeli hale gelme potansiyeline sahiptir (Aytekin, 2015). Özellikle devletlerin sırları ve özel bilgilerini ele geçirmek için yürütülen siber saldırılar adeta bir savaşa dönüşmüştür (Aslay, 2017). Bu yüzden ülkelerin savunma sistemlerinin kapsamında siber güvenlik politikaları ve siber güvenlik sistemleri de artık devlet savunma sisteminin bir parçası haline gelmiştir.

Bu bağlamda literatürde yer alan çalışmalar ve kamu kurumlarının bir nevi devletlerin siber güvenlik raporları incelendiğinde durumun ehemmiyeti ortaya çıkmaktadır. Bu açıdan siber güvenlik ile ilgili yapılan bu tez çalışmasının literatüre önemli katkılar sağlayacağı düşünülmektedir. Çünkü tezde literatürdeki diğer çalışmalardan farklı olarak dünya ve Türkiye'de gerçekleşen güncel tüm siber saldırı vakaları sistematik ve kapsamlı bir şekilde incelenmiş ve tablolar şeklinde listelenmiştir. Böylelikle bir okur, uzman ya da araştırmacı güncel saldırı vakalarını ve bu saldırıların tüm özelliklerine bu tez çalışmasından ulaşabilecektir. Ayrıca yoğunlukla kullanılan siber saldırı türlerinin tespit edilmesi, bu saldırılara karşı alınacak önlem ve farkındalık açısından da önem arz etmektedir. Türkiye'de siber güvenlik konulu yürütülecek akademik çalışmaların kapsamını genişletmesi,

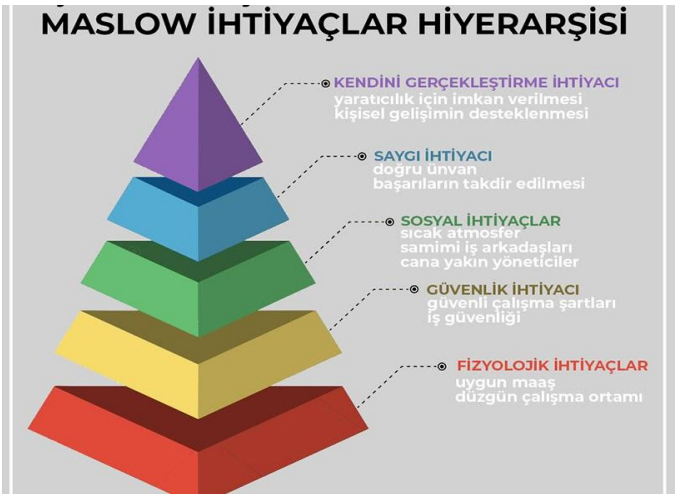
literatürdeki yeni yürütülecek çalışmalara yön vermesi ve Türkiye'de siber güvenliğin hem bireyler hem de devlet açısından önemini vurgulaması bu tezin önemi ve öz değerinin bir göstergesidir. Son olarak, unutulmamalıdır ki; siber ortamda gerçekleşen saldırıların sadece resmi kurum ve kuruluşları değil, şahısları da direkt olarak tehdit etmektedir ve Türkiye'nin en fazla tehdide ve siber saldırıya maruz kalan ülkeler arasındadır (Altun, 2022). Bu açıdan siber saldırılar ve güvenlik ile yürütülen bu çalışmanın bulguları ülkenin güvenliği açısından da önem teşkil etmektedir.

Tez çalışmasında bütünsel açıdan "Siber güvenlik" kavramı ele alınmıştır. Bu kavram üzerinde kapsamlı bir veriyi içeren bu tez 6 bölümden oluşmaktadır. Birinci bölümde tezin amacı, önemi ve literatür açısından özgün değeriyle birlikte giriş yapılmıştır. İkinci bölümde siber güvenlik ile ilgili siber uzay, siber alan ve siber suçlar gibi kavramlar ve tanımları açıklanmıştır. Üçüncü bölümde mühendislik açısından temel siber saldırı türleri, saldırı türlerinin işleyiş mekanizmaları ve verdikleri zararlar üzerinde durulmuştur. Dördüncü bölümde siber saldırılara karşı alınan güvenlik önlemleri, politikalar ve son kullanıcılar için gerekli tedbirler işlenmiştir. Beşinci bölümde ise dünya ve Türkiye'de yaşanmış olan güncel ve etkili siber saldırı vakaları incelenmiş ve bu saldırılarda kullanılan saldırı türlerinin yılı, hedefi ve türü gibi bilgileri içeren bir sınıflandırılması yapılmıştır. Son olarak altıncı bölümde ise yürütülen tezde siber güvenlik ve siber saldırı türleri ilgili elde edilen bulgular neticesinde sonuçlar ortaya konulmuş ve literatür üzerinden tartışma yürütülmüştür.

BÖLÜM 2

SİBER GÜVENLİK

Siber güvenlik kavramına geçmeden önce güvenlik kavramı ve güvenlik ihtiyacının doğuşundan söz etmek yerinde olacaktır. Güvenliğin tarih boyunca tüm insanlığın en temel gereksinimleri arasında yerini aldığı söylenebilmektedir. Güvenlik, günlük hayatın bir parçası olarak, barınma, yeme-içme, korunma ve psikolojik olarak güvende olma hissi de dâhil olmak üzere pek çok şeyi içermektedir (Bakrania ve Haider, 2016). Buna örnek olarak Abraham Maslow'un ihtiyaçlar piramidi verilebilmektedir. Bu piramitte de güvenlik ihtiyacı tüm fizyolojik ihtiyaçlardan önce gelmektedir. Tarihin seyri boyunca değişen ve farklı şekillerde karşımıza çıkan güvenlik kavramı teknolojinin ilerlemesi ve gelişmesi ile farklı bir boyuta taşınmıştır.



Şekil 2.1. Maslow'un İhtiyaçlar Hiyerarşisi (Jerome, 2013)

ABD'li psikolog Abraham Maslow, insan için çok önemli olan güvenlik ihtiyacını yukarıdaki piramitle açıklamaya çalışmıştır. İnsan için ilk olarak fizyolojik ihtiyaçlarını oluşturan yeme-içme, uyuma gibi fizyolojik ihtiyaçları oluşturmaktadır (Jerome, 2013). Bu temel ihtiyaçlarını gideren insan, bir sonraki aşama olan karşısına çıkabilecek tehlikelere karşı korunmak, önlem almak, varlığını sürdürebilmek, kısacası güvenliğini sağlamak istemektedir. Buradan şu sonucu çıkarmamız mümkün görünmektedir. Kişi, sevgi, saygı, aidiyet, kendini gerçekleştirme vb. ihtiyaçlarından önce güvenlik ihtiyacını sağlamak istemektedir. Buradan güvenlik kavramının insan hayatı için ne derece mühim bir kavram olduğu sonucu çıkartılabilmektedir. Bu uğurda kişiler tarihte pek çok kez temel hak ve hürriyetlerinden güvenlik ihtiyacı uğruna vazgeçmişlerdir (Ünver ve Canbay, 2010). Tüm bunlar meydana gelirken insanlar kendi güvenliklerini sağlayabilmek için ordu, polis gibi teşkilatlar kurmuş ve güvende olmaya çalışmışlardır. Şu an içinde bulunduğumuz yüzyılda teknolojik, ekonomik, politik, sosyal alanlardaki inanılmaz değişimler geleneksel güvenlik anlayışını yetersiz kılabilmekte olduğu düşünülmektedir.

Güvenlik kavramı Türk Dil Kurumuna göre ; "*İnsanların hayatında yasal düzen ve ilişkinin bir problem olmadan yürümesi, bireylerin korkmadan ve güvenli hissederek yaşayabilmesi durumu*" şeklinde tanımlanmaktadır (Türk Dil Kurumu). İnsanın varoluşundan bu yana toplumsal yaşamın bir zorunluluğu olarak karşımıza çıkan güvenlik kavramı kişinin varlığının koruma ve devam ettirebilmesinin zorunlu bir durumu olan olgu olarak karşımıza çıkmaktadır. Başka bir tanım da ise güvensizlik risklerinin ortadan kaldırılması şeklinde karşımıza çıkmaktadır ayrıca tehlike ve risk kavramları ile birlikte ifade edilmektedir. Özellikle halk arasında kullanılan "savunma" kavramının yerine de sık sık kullanılmaktadır. Güvenlik kavramı en özelden yani aileden topluma, toplumdan devlete, devletten ülkeye kadar çok geniş seviyelerde karşımıza çıkabilmektedir.

İnsan eliyle ortaya çıkarılan siber uzay her an genişlemeye ve insanların hayatında daha çok yerini almaya başlamıştır. Bu durumun siber güvenlik kavramını ortaya çıkardığı söylenebilmektedir.

Siber güvenlik kavramı 1970'li yılların başında ABD'de ortaya çıkan ve 1990'lı yılların sonlarına doğru diğer ülkelerde yaygınlaşmaya başlayan teknolojik gelişmelere istinaden ve özellikle de soğuk savaş sonrası ortaya çıkan coğrafi değişim ve gelişmelere bir yanıt olarak ortaya çıktığı düşünülmektedir. İlk ortaya çıktığında insanların endişeleri sadece devletlerin bilgi sistemlerinde bulunan gizli bilgilere ulaşılmasına ilişkin idi. Daha sonları bilgisayar ağlarının büyümesi ve her geçen gün günlük yaşamımıza daha fazla entegre olmasıyla birlikte ana temeli de farklılaşmıştır. Siber güvenlik, terim olarak bilgisayar hakkında araştırmalar yapmaya başlayan araştırmacılar tarafından 1990'lı yılların başında kullanılmaya başlanmıştır. İlk başlarda sadece ağ bağlantılarını içeren bir dizi güvensizliği belirten siber güvenlik kavramı, daha sonraları teknik bilgisayar güvenliği anlayışının ötesine ulaşarak tüm ulusların refah seviyesi, güvenliği, ekonomisi üzerinde sanal tehlikelerden doğan, keskin toplumsal sonuçlar yaratabileceği noktasına doğru biçim almıştı (Adams vd., 2015). Siber güvenlik kavramı, internetin günümüzde casusluk, siyaset ve askeri faaliyetler için bir araç ve iş dünyası için küresel bir altyapı olarak geliştirilmesi ile beraber ulusal ve uluslararası güvenlik için merkezi bir konu haline bürünmüştür (Klimburg vd., 2011). Verilen bu kısa bilgilerden sonra aşağıda siber güvenlik kavramının tanımı ve gelişimiyle konu daha da aydınlatılmaya çalışılacaktır.

Siber güvenlik kavramı için üzerinde uzlaşma sağlanmış bir tanım mevcut değildir. NICE (The National Initiative for Cybersecurity Education) siber güvenliği; "*Bilgi ve teknoloji süreçleri ile bu süreçlerde bulunan bilgilerin herhangi bir sa*ldırı, ziyan ve heba etme, yok etme gibi durumlara yönelik olarak tedbir alınan bir durum olarak" tanımlanmaktadır. Uluslararası telekomünikasyon birliği ise siber güvenlik kavramını; "*siber doğa, müesseseler ve kişilerin mevcudiyetlerini sağlamak için kullanılabilecek malzemelerin, politikaların, güvenlik olgularının, güvenlik talimatlarının, risk yönetim yaklaşımlarının, hareketlerin en iyi örneklerin, güvence ve teknolojilerin toplamı*" olarak tanımlamaktadır (Paulsen vd., 2012).

Siber güvenlik kavramından söz edecek olursak bu kavramın doğuşu bilgiye ulaşma ve onu elde etme doğamızdan dolayı ortaya çıkmıştır. 21. yüzyılda teknolojinin bu denli hız kazanıp hayatımızın içine entegre olup sağladığı birçok yenilik ve kolaylığın yanı sıra, ortaya

çıkardığı olumsuz etkileri de kimi zaman gözlemleyememezine sebep olmaktadır. Siber güvenlik siber alanda müessese, kuruluş ve kullanan kişilerin mevcudiyetlerini korumak amacıyla kullanılan araçlar, politikalar, kılavuzlar, güvenlik politikaları, eğitim ve teknolojiler, faaliyetler bir bütün olarak açıklanmaktadır. 2016-2019 yılları arasında yayımlanan Ulusal siber güvenlik stratejisi belgesinde siber güvenlik şu şekilde tanımlanmıştır: "*Siber ortamı meydana getiren bilgisayar ağlarının her türlü saldırılardan önlenmesini ve o çevrede ortaya çıkan bilgilerin gizlice, bütün olarak ve işbirlikli olarak güven altında olmasını, yapılan saldırıları ve siber güvenlik durumlarının ortaya çıkarılmasını bu durumlara karşı tespit kanallarının oluşturulmasını ve kullanılmasını ve daha sonra ise sistemlerin ömrünü siber güvenlik sorunu yaşamadan önceki haline getirmeye çalışılmasını ifade etmektedir*" (Çiftci, 2017).

Teknolojiye olan bağımlılığımız arttıkça, ortaya çıkaracağı zayıflıklar, açıklıklar ve olumsuz tarafları da bir hayli çok olacaktır (Cavelty, 2008). Bilgi ve iletişim teknolojilerindeki yaşanan bu hızlı değişim ve gelişimler, bu mekanizmalar sayesinde bizlere sağlanan hizmetlerin hayatımızın her alanında yaygınlaşmasının sonucunda bilgi ve iletişim teknolojilerinin hayatımızın her alanında oynadığı rolün artış gösterdiği düşünülmektedir. Siber güvenlik kavramı ile kişinin kendisi dâhil olmak üzere diğer varlıkların da korunmasının kapsandığı söylenebilmektedir. Siber güvenlik terimi ile bilgi güvenliği terimi birbirlerinin yerine kullanılan kavramlardır. İki kavram da birbirleriyle örtüşmesine rağmen aralarında anlam farkı bulunmaktadır. Siber güvenlik sadece bilgi kaynaklarının korunmasını değil aynı zamanda kişinin kendisini ve diğer varlıkları da kapsayarak geleneksel bilgi güvenliğinin dışına çıkmaktadır (Solms ve Niekerk, 2013). Siber güvenlik yalnızca internet güvenliği değil, tüm iletişim altyapılarını kapsayan ve koruyan bir kavram olarak karşımıza çıkmaktadır (Hekim ve Başıbüyük, 2013).

Siber güvenlik kavramını en genel şekli ile ifade edecek olursak; 21. yüzyılın uluslararası iktisadına etki eden ve onu hareketlendiren önemli zeminlerin korunmasının yanı sıra hem devlet gizlerinin hem de ulusal savunmanın oluşturulması için önem taşıdığı düşünülmektedir (Klimburg ve Tirmaa-Klaar, 2011).

2.1. Siber Güvenlik ve Savunmanın Önemi

Siber güvenlik terimi ilk olarak 1990 yılında bilgisayar mühendisleri tarafından, ağa bağlı bilgisayarlarla ilgili güvenlik açıklarını ortaya çıkarmak için kullanılmıştır (Lene Halsen, 2009). 31 Ocak 2019 itibariyle dünya nüfusunun yarısından fazlasının internete ulaşımı mevcuttur (Hootsuite, 2019). İnternetin ağının gelişmesiyle büyüyen siber tehditler bilgini güvenliği kavramını ortaya çıkarmıştır. Siber alanın emin ve güvenli kalabilmesi açısından bilgi güvenliği yönetim sistemi standardında olduğu gibi bilginin gizliliği, bütünlüğü ve erişilebilirliğinin sağlanması gerekmektedir (M. Goodrich, 2010).

Siber saldırılar yalnızca bilgisayar kanallarına vermiş oldukları zarar dışında bir ülkenin kilit sahaları olan iletişim sistemi, enerji ve ulaşım ağı, bilgisayar sistemleri, askeri komuta ve kontrol sistemlerine zarar verebilecek ölçüde bir savaş çeşidi olarak da ortaya çıkmaktadır. 2007 yılında Rusya tarafından Estonya'ya yapılan siber saldırılar tüm devlet kurumları, haber kanalları ve finans kuruluşlarının internet sitelerini düzenlenen bu girişim ilk kez sistematik olarak yapılan siber savaştır (Siber Bülten, 2015). Yaşanan bu olay siber saldırılar, önümüzdeki yıllarda önemli bir tehdit unsuru olarak dünya tarafından kabul edilmeye başlanmıştır. Sözü edilen bu siber saldırılar, tüm ülkelerde suç başlığı adı altında yer almaktadır.

Sürekli artan dünya nüfusuna paralel olarak internete ulaşımın muazzam bir hızla artması; siber alanların büyümesi ve farklılaşması bu alanlardaki güvenlik önlemlerini de gittikçe zor kılmaktadır. Tam anlamıyla başarılmış görülebilecek bir siber güvenlik oluşumu ve sistemi, bilgisayarlarda, bağlantılarda, verilerde, ya da güvende olunması istenilen hiç fark etmeksizin bir veri topluluğunda bile olabilen ve yayılmış çeşitli koruma kalkanlarına sahiptir.

2.2. Siber Güvenlik Kavramı ve İlişkili Tanımlar

Son yıllarda bilgi teknolojilerindeki inanılmaz hızlı değişim ve gelişim beraberinde bazı tehlikeli olabilecek durumları da ortaya çıkarmıştır. Bilgisayarın icat edilmesi sonrası teknolojinin bu denli gelişmesi ile doğru orantılı olarak bilişim sistemleri insan yaşamının

bir parçası haline gelmiş bulunmaktadır. Bu gelişmeler doğrultusunda ihtiyaçlar, tehdit, risk ve birtakım tehlikeler karşısında bu durumlardan korunmak ve önlem alabilmek için siber ortamın güvenliği kapsamında yeni kavramlar ve tanımlar şekillenmeye başlamıştır. Bu terim ve kavramların yeni olmasından dolayı çok çeşitli tanımlarının bulunduğu ifade edilmektedir. Bu tanımlardan biri de Siber güvenlik olarak karşımıza çıkmaktadır. Krämer tarafından yapılan bir araştırmada siber güvenlik teriminin 28 farklı tanımı olduğu ifade edilmiştir (Krämer vd., 2011). Siber güvenlik kavramının geniş ve ayrıntılı bir biçimde ele alınması analiz edilmesi ve yorumlanmasının anlaşılabilmesi açısından öncelikle bu konu ile alakalı kullanılan terimleri bilmek, anlamak, konu ile alakalı ortaya çıkan gelişmeleri takip edebilmek, aynı dili konuşmak ve anlamak kadar önemli bir durumdur. Siber güvenlik kavramı ile iç içe geçmiş terim ve kavramlar şu şekilde sıralanabilmektedir. Bu kavramlar; Siber kavramı, güvenlik, siber alan, siber uzay, siber güvenlik, olarak karşımıza çıkmaktadır.

2.3. Siber Kavramı

Siber güvenlik kavramına geçmeden önce "Siber" kelimesinin anlamını açıklamanın faydalı olacağı düşünülmektedir. Siber kavramı bilgisayar ve ağlarını içeren bileşenleri ve durumları tanımlamak için kullanılmaktadır. Türk Dil Kurumu'na göre "Siber" kelimesi, "*Bilgisayar ağlarını içeren internete ait olan, sanal gerçeklik gibi terimlerle ifade edilmektedir*" (Türk Dil Kurumu, 2021).

Bilgisayar bilimi alanında kullanılan siber sözcüğünün İngilizcedeki karşılığı "cyber" dir. Cyber kavramı Yunanca' da hükmetmek ve yönetmek anlamlarına gelmektedir. Bu terim ilk defa Louis Couffignal tarafından kullanılmıştır. Couffignal, 1958 yılında canlılar ve makineler arasında bulunan telekomünikasyon bağlantısını incelemiştir. Ayrıca da Sibernetik biliminin babası olarak bilinmektedir (T.C. Sağlık Bakanlığı, 2014). Siber kelimesinin ortaya çıkışından itibaren içerisine aldığı unsurlar ve kavramlar günden güne farklılaşmaktadır.

İçinde bulunduğumuz yüzyılda siber sözcüğü içinde bulunduğu her sözcüğe bilinenden öte anlamlar yüklemekte ve kendine özgü komplike yapısı ile özgün özelliklere sahiptir. Bilgisayar ve iletişim unsurlarını içine alan ve yeniden düzenleyen bir sistem olduğu düşünülmektedir. Ayrıca siber uzayın, verileri saklayan bilgisayarlara ek olarak bu veri

akışlarını sağlayan sistem ve altyapıları bir bütün haline getirerek sanal dünyayı ve fiziksel dünyayı tek bir çatı altında topladığı düşünülmektedir. Siber sözcüğünün köken bilimi incelendiğinde yakın zamanlarda tanımlanan ve anlam kazanan durumundan bir hayli uzaklarda ve farklı alandan ortaya çıktığı görülmüştür.

Siber ifadesinin eski Yunan döneminde Kübernetes olarak kullanıldığı ifade edilmektedir. Sibernetik kelimesinin ön ekini oluşturan siber kavramı ise kelime manasına bakıldığında bilgisayar ve elektroniği içinde barındıran teknolojileri kapsamaktadır (Nye, 2011). Günümüzde ise altyapısı bilişim sistemleri olan ağlar olarak tanımlanmaktadır.

Siber kavramından sonra aşağıda siber alan kavramı açıklanmaya çalışılacak olup literatür ışığında bilgiler verilmeye çalışılacaktır.

2.4. Siber Alan

Küreselleşme ile birlikte içinde bulunduğumuz çağda bilgi teknolojileri alanının devrimsel bir değişime uğradığı söylenebilmektedir. İnternetin icadı, bilgisayarların boyutlarının küçülmesi buna paralel olarak özelliklerinin her geçen gün artması, sosyal paylaşım ağlarının ulusal sınırları aşarak toplumlar arası etkileşime sebep olması, tüm bunlarla ilişkili olarak yığınların kitlesel seferberliğinin artması ve dolayısıyla kontrol edilebilirliklerinin azalması gibi olaylar bahse konu olan gelişmelerin örneklerindendir. Tüm bunlardan hareketle artık 21. yüzyılda siber alan kendini genişletmesinin haricinde artık fiziksel alanları bile etkiler hale geldiği söylenebilmektedir.

Siber Alan kavramı ile ilgili olarak günümüzden örnek verilecek olursa, banka işlemlerini, iletişimi ve e-devleti kendisine bağlı bir yapıda olmayı doğurmuştur. Bundan dolayı siber alanın büyümesi ve kapsadığı alanın artması, konunun Uluslararası İlişkiler disiplini içerisinde değerlendirilmesini gerekli kılmıştır. Daha önce de söz edildiği üzere siber alan, küreselleşme ile ilişkilendirilerek ülke bağımsızlığını ve dolayısıyla uluslararası ilişkileri etkisi altına aldığı düşünülen olaylar ile karşılaştırıldığında sanal olmasının yanı sıra bu alanda reel bir etki yaptığı söylenebilmektedir. Şimdi de siber alan deyimiyle ne anlatılmak istendiğine değinmek yararlı olacaktır. Siber alan kavramı ile temelde ve ortaya

çıkmasında bilgisayar olan sanal dünya tanımlanmaktadır. Başka bir ifade ile siber alan, bilgisayarın ortaya çıkması ile başlayan ve günümüzde gerçek alanları bile etkisi altına alan sanal âleme dayanmaktadır.

Bunların yanında kavramın tanımında dikkat çeken birkaç önemli nokta yer almaktadır. Birinci sırada kavram sanal yani gerçek dışını ifade etse de aslında ortaya çıkardığı etki açısından tamamen gerçektir. İkinci olarak, siber alan gerçek dünyadaki durumu asimetrik olarak arttıran bir yapıya sahiptir. Bunu açıklamak gerekirse; gerçek dünyada etkinliği ve yetkinliği oldukça az olan bir birey, sanal ortamda siber alanda yaptıkları sayesinde etkinliğini ve yetkinliği ortaya çıkartabileceği ve bunu katlayabileceği düşünülmektedir. Son ve olumsuz olan çıktısı ise, siber alanın gerçek kimlikleri devre dışı bırakmasıdır. Gerçek dünyadaki hukuki sorumluluk ve yaptırımların sekteye uğradığı bir alandır.

2.5. Siber Uzay

Siber alan kavramından sonra siber uzay kavramına değinmek yerinde olacaktır. Siber uzay kavramının mimarı olan Gibson, siber uzayı 1982 yılında yayınladığı kısa hikâyede karışık varyasyonları içeren teknik bir terim olarak tanımlamıştır. 1984 yılında yayınladığı Neuromancer isimli romanında bu kavrama değinmiştir. Romanda siber uzay kavramını daha büyük alanda ve teknik anlamda milyarlarca ağ tarafından birbirleri ile karşılıklı olarak iletilen iletilerin insan beyninde canlandırılması zor olan ve son derece komplike olan grafiksel bir alan olarak tanımlamıştır (Heylighen ve Cliff, 2001). İngilizcede "cyberspace" olarak ifade edilen bu kavram, dilimize siber uzay, siber alan, siber ortam olarak girmiştir (Tureng Sözlük, 2014). Siber uzay iletişim unsurları, bilgisayar sistemleri ve kontrol birimlerinden oluşan, bilgi ve teknoloji altyapılarından meydana gelen ve birbirlerine bağımlı ağlardan oluşan ve herhangi bir coğrafi sınırlamaya maruz kalmayan uluslararası bir bilgi ortamıdır. Bir zamanlar yalnızca iletişim amaçlı olarak kullanılan siber uzay, 21. yüzyılda ise, bankacılık, haberleşme, ulaşım, sağlık, eğitim ve enerji tesisleri gibi daha birçok kritik alanda kendisine bir yer bulduğu söylenebilmektedir. Siber uzay kavramı 1990'lı yıllarda uzmanlar tarafından "*bilgisayar ile devam ettirilen, ulaşılan ve üretilen*

uluslararası ağ bağlantılı sanal ve yapay iletişim alanı" olarak tanımlanmıştır (Benedikt, 1991).

İnsanoğlunun varoluşundan bu yana zaman içerisinde kendine has özellikleri ve şartları bulunan dört savaş alanına (kara, deniz, hava, uzay) 21. yüzyıla geldiğimizde bu alanları kapsayan ve 5. hareket alanı olarak isimlendirilen "siber uzay" (siber ortam, sanal ortam, sayısal ortam, bilgi ortamı vb.) kavramı eklenmiştir. Tanım olarak bakılacak olursa siber uzayın zaman içerisinde pek çok farklı şekilde tanımının yapıldığı görülmektedir. En geniş tanımı ise Singer ve Friedman tarafından yapılmıştır. Bu tanım ; "*bilgisayarlardan, füzelere, füzelerden güneş ışınlarına kadar elektromanyetik yörüngenin kullanılması ile ifade edilen yer*" olarak tanımlanmıştır (Singer ve Friedman, 2015).

Türkiye 2016-2019 Ulusal Güvenlik Stratejisi belgesinde siber uzay şöyle tanımlanmıştır; "*Tüm dünyaya ve uzaya erişmiş konumda olan bilgisayar ve ağ sistemlerinden meydana gelen ve bunların arasındaki iletişimi sağlayan ağlar ve bilgi sistemlerinden meydana gelen alan*" olarak tanımlanmaktadır. Bu tanımlara bakıldığında siber uzayın fiziksel ve sanal yapı olarak iki birleşik yapıdan oluştuğu görülmektedir.

Fiziksel yapının bileşenleri şunlardır; bilgisayarlar, akıllı telefonlar, akıllı nesneler, sayısal elektronik nesneler, algılayıcılar, uydu sistemleri, internet / bilgisayar ağları olarak karşımıza çıkmaktadır. Sanal yapının bileşenleri ise; İşletim sistemleri, veri tabanı yönetim sistemleri, yazılım ve kodlar ile üretilen, depolanan ve iletilen çeşitli maksatlarla kullanılan her türlü verileri ve bilgileri içermektedir.

İçinde yaşamış olduğumuz bilgi çağında siber uzay artık yaşamımızın vücudumuz ve beynimiz gibi bir parçası haline gelmiştir. Hal böyle iken, siber tehdit ve riskler, siber saldırılar, siber terörizm, siber savaş gibi pek çok olumsuz durumu da beraberinde getirmekte olup bu liste her geçen gün çeşitlenerek çoğalmaktadır.

2.6. Siber Suçlar

Bilgisayarların hem iş hayatında hem de özel hayatımızda çok fazla yer almasından dolayı klasik suç tanımına uymayan ve bilgisayar ve bilişim suçları olarak karşımıza çıkan suçlar siber suçlar olarak adlandırılmaktadır. Genel olarak "*bilgisayarların art niyetli ve kötü amaçlar için kullanılması, bilgilerin otomatik kayıt altına alındığı ve verilerin transferine ilişkin yasaya ve meslek ahlakına aykırı durumlar*" şeklinde tanımlanmaktadır.

Avrupa Konseyi (AK) Siber Suçlar Sözleşmesi (2004)' nde ise; izinsiz erişim, sisteme veya veriye müdahale, bilişim sistemleri vasıtasıyla dolandırıcılık veya sahtekârlık suçlarının yanında, özellikle son dönemlerde artan internet ve bilgisayar kullanımı yanında, niceliksel olarak ortaya çıkan çocuk pornografisi, telif haklarına ilişkin ihlaller, ırkçılığın ve yabancı düşmanlığının önlenmesine ilişkin hükümler de siber suçlar kapsamındadır. Siber suçlar ile alakalı yasalar ve düzenlemeler ülkeden ülkeye göre değişiklik göstermektedir.

Genel olarak bilişim ve bilgisayar sistemleri üzerinde kişi, kişiler ve organize suç örgütleri tarafından siyasal amaçlar hedeflemeyen ve ulusal güvenlik açısından problem olarak görülmeyen siber saldırılar ve hukuka aykırı fiiller siber suç olarak kabul edilmekte ve yasalar karşısında buna göre işlem görmektedir. Her türlü siber saldırı ve olayların terör unsurlarınca veya terör maksatlarıyla gerçekleştirilmesi durumunda ise siber terörizm şeklinde ortaya çıktığı görülmektedir. Siber Saldırı konusu ayrı bir başlık altından ikinci bölümde anlatılacağından bu bölümde değinilmemiştir.

2.7. Siber Riskler ve Tehditler

Siber tehditler, siber ortamda kişisel ve kurumsal bilgilerin ve verilerin gizliliğini yasal olmayan yollara başvurarak bunlara ulaşmak ve bu bilgi ve verilere zarar vermek ve tahrip etmek maksadı ile yapılan her türlü saldırının genel adı olarak ifade edilmektedir (Şahinaslan, 2003). Bilgi sistemlerinin günden güne gelişmesi ve ilerlemesi siber alanda bir takım tehditleri de doğurmaktadır. Bu tehditler hem devlet hem de devlet dışı faktörler için risk durumunu oluşturmaktadır. Özellikle bu tehditlerin soyut alandan geliyor olması, tehditlerin sonuçlarının öngörülebilirliği açısından bir dezavantaj durumu oluşturmaktadır.

Tehditler yerlerine göre iç ve dış tehditler olarak sınıflandırılmaktadır. Kaynaklarının insan olmasına göre kötü niyetli olan ve kötü niyetli olmayan şeklinde gruplandırılmaktadır (Kurnaz, 2016).

Kötü niyetli olan durumlar; Zarar vermek veya çıkar sağlamak amaçlı ağ saldırısı, zararlı yazılım yüklemesi, yetkisiz erişim vb. olarak sınıflandırılabilmektedir. Kötü niyetli olmayan durumlar ise; Eğitimsiz, bilinçsiz, dikkatsiz kullanıcılar tarafından yanlış veri girişi, zararlı yazılım yüklemesi vb. olarak sınıflandırılabilmektedir. Ayrıca doğal kaynaklı olarak uzun süre elektrik kesintisi, sel, hava kirliliği, yıldırım düşmesi, toprak kayması vb. etkenlerle meydana gelen olayları da örnek olarak gösterebilmektedir. Siber riskler ise, Tehditlerin bilgi varlıkları üzerindeki açıklıklarını kullanarak zarar yaratma potansiyeli şeklinde tanımlanmaktadır (Sağıroğlu, 2018). Ulusal siber güvenlik strateji belgelerinde yaygın olarak kabul edildiği görülen riskler şunlardır (UDHB, 2016);

- Toplumun sosyal ağlara bağlılığı,
- Kritik kurum ve kuruluşların siber uzaydaki konumu
- Çeşitli siber casusluk çalışmaları ve hedefli saldırılar
- Kurumlar arası koordinasyon eksikliği
- Personel ve yetkinlik bağlamında yetersizlik olarak sıralanabilmektedir.

2.8. Siber Terörizm

En basit ifade ile siber uzay ve terörizm ifadelerinin birleşiminden meydana gelmektedir. Terör örgütlerinin siber ortamdan yararlanarak terör faaliyetlerini meydana getirmesi şeklinde ifade edilebilmektedir. Teknolojinin her geçen gün gelişmesi ve siber ortamda kullanımının artmasıyla, terör gruplarında da bu teknolojiler kullanılması artış göstermektedir.

Günümüzdeki terör grupları, örgütlerinin, yapılandırmak, örgüte yeni insanlar kazandırmak, eylemlerini ve organizasyonlarını gerçekleştirmek maksadıyla bilgi ve bilişim sistemlerini yaygın olarak kullanmakta ve özel ve kamu kurum ve kuruluşlarının bilişim sistemlerini hedef alan saldırılar gerçekleştirdikleri görülmektedir.

Uluslararası mecralarda terörizmin tanımının olmadığı gibi siber terörizmin de kabul görmüş ortak bir tanımı bulunmamaktadır. Siber terörizmin ortak bir tanımı yapılacak olursa; "*siyasal ve sosyal hedefleri başarmak, insanları ve devleti korkutmaya çalışarak baskı oluşturmaya çalışarak etkilemek, devlet politikalarını değiştirmeye çalışarak, bilgisayarlara ağ sistemlerin, veri tabanlarına, bilişim teknolojilerinin unsurlarını kullanarak yapılan kanun dışı ve zarar verici saldırılar*" olarak tanımlanmaktadır.

Siber terör olaylarında, bilişim sistemleri aracılığıyla kişilere, devlete, kurumlara yapılan terör saldırıları korku ve şiddet içermesinin yanı sıra can ve mal kayıplarına da sebebiyet verebilmektedir. Bu yüzden önem arz etmektedir.

2.9. Kritik Altyapı

Bir devletin fiziksel ve sanal ortamda verdiği hizmetler; bilgi iletişim teknolojileri, su ve enerji kaynakları, kimya, uzay ve nükleer endüstri, sağlık, ulaşım, bankacılık ve finans gibi birçok kamu hizmetinin tümünü oluşturan yapıya kritik altyapı denilmektedir.

Kritik altyapıların en önemli özelliği; devletin ve toplum için hayati öneme sahip ağların yönetildiği bu sistemlerin kesintisiz olarak hizmet sağlayabilmesidir.

BÖLÜM 3

SİBER SALDIRILARI TÜRLERİ

Günümüz teknoloji çağının yaygın sorunlarından siber saldırılar dünya çapında tüzel kişileri, özel şirketleri ve devletlerin kurumlarını zor durumda bırakmaktadır. Özellikle son zamanlarda tüm işlemlerin elektronik ortamda gerçekleşmesi yüzünden siber saldırıların sayısı günden güne artmaktadır. Siber saldırılar farklı yöntemlerle yapılmaktadır. Literatürde birçok siber saldırı türü üzerinde durulmaktadır. Bu bağlamda tezin bu bölümünde siber saldırı türleri incelenecektir.

3.1. Kötü Amaçlı Yazılımlar (Malware Software)

Kötü amaçlı yazılımlar başka bir ismi ile "Malware" tanım olarak kötü niyetli tüm yazılımlara verilen ortak bir tanımlamadır. İngilizce olarak "malicious software" kelimelerinden doğmuştur. Bu yazılımlar kapsamında solucanlar, virüsler, fidye yazılımları, truva atları, casus yazılımları ve reklam yazılımları vb. bulunmaktadır. Bu yazılımların temel mantığı kişilerin izni olmadan bilgisayar sistemlerine sızmaktır. Bu yazılımlar sayesinde saldırganlar;

- Bilgisayar sistemlerinin çalışması durdurulabilir,
- Gizlenerek, casusluk faaliyeti yürütülebilir,
- Çoğalarak olumsuz etkiyi artırabilir,
- Sistemlere erişim izni vererek uzaktan sistemleri kontrol edebilmektedirler,
- Önemli verilerin çalabilir, şifreleyebilir, silebilir, temel fonksiyonları değiştirebilirler (Ye vd., 2008; Shabtai vd., 2009).

Kötü amaçlı yazılımların birçok türü vardır. Bu türlerin farklı özellikleri ve amaçları bulunmaktadır (Canbek ve Sağıroğlu, 2006; Tokmak ve Küçüksille, 2019)

3.1.1 Fidye Yazılımı Saldırıları (Ransomware)

Fidye yazılımları (Ransomware), siber hedefteki kullanıcının sistemine ya da bilgisayarına sızarak önemli verilerin şifrelenmesi için tasarlanmıştır. Böylelikle siber suçlular bilgisayarı kilitleyerek eski durumuna getirilmesi için bir fidye talep etmektedir. Fidye yazılımlarının sisteme girişi şu şekilde olmaktadır. İlk olarak kötü amaçlı yazılım cihaza erişim elde eder. Fidye yazılımının türüne bağlı olarak, işletim sisteminin tamamı ya da belirli dosyalar şifrelenebilir. Nihayetinde siber kurbanlardan bir fidye talep edilmektedir. Genellikle literatürde en çok rastlanan iki tür fidye yazılımı olduğu görülmektedir. Bunlar kilitleyici fidye yazılımı ve şifreli fidye yazılımıdır. Bu ikisi arasındaki fark *kilitleyici fidye yazılımı* temel bilgisayar işlevleri etkilerken iken *şifreli fidye yazılımı* belirli dosyalar şifrelemektedir (Kaspersky, 2020). Fidye yazılımının bulaşma önlemleri incelendiğinde ise en sık rastlanan üç yaklaşım; e-postalar, yazılım açıkları ve sunuculardaki güvenlik zaaflarıdır (Turhost, 2021).

Fidye yazılım türleri birden çok olmasına rağmen en çok bilinen türleri Leakware veya Doxware'dır. Bu yazılım türleri ise şirketlerin gizli dosyalarını şirketlere karşı internet üzerinden yayınlamakla tehdit için kullanmaktadır. Sayıları sürekli günden güne artmakta olan fidye yazılımlarını veri sabote işlemlerinde en çok rastlanan fidye yazılım türleri şunlardır (Coveware, 2020):

- *REvil (Sodinokibi):* Tespiti gerçekten zor olan bir tür olarak bilinir.
- *Labirent:* Veri hırsızlığı yaparak, verileri satmakla tehdit eder.
- *Phobos:* Üretkenlik belgelerini kilitlemektedir.

Fidye yazılımları daha eskilere dayanmasına rağmen 2005 yılında Rusya'da görülmüştür. O tarihten bu yana fidye yazılımları dünyaya yayılmıştır. İstatistiklere göre 2011 yılında, fidye yazılımı saldırılarında büyük bir artış gözlendiğini rapor etmektedir. Fidye yazılımları günden güne de artmaktadır. Bu açıdan fidye yazılımlarını engellemek ya

da minimum zarar için, önceden verileri yedeklemek ve güvenlik yazılımları kullanmak gerekmektedir (Kaspersky, 2020).

3.1.2. Solucanlar ve Kurtçuklar (Worms)

Siber saldırılar türlerinden biri olan solucan (worm) virüsler siber saldırı ataklarının ilk türü olan "basit ve yapılandırılmamış" kategoride yer almaktadır. Solucanlar, genellikle hedef gözetmeksizin, çok hızlı ve etkili bir şekilde yayılarak işlemci hızını düşürmek, interneti yavaşlatmak gibi sonucunda büyük zararlar verebilmektedirler (Kınay, 2012). Son yıllarda bu virüslerin birçok saldırıda kullanıldığı görülmektedir (Holat, 2021). Solucanlar tasarım ve yapı olarak virüslere çok benzemektedir. Fakat solucanların, virüslerden farkı insan etkenine gereksinim duymadan sistemlere bulaşabilmeleridir (Ulaşanoğlu vd., 2010). Bilgisayar eğer bir ağa bağlı ise bunu anlar ve o iletişim ağında bulunan diğer bilgisayarlara saldırı düzenler bir nevi kartopu örneklemi şeklinde ilerler. Solucanlar işletim sistemindeki dosya iletim özelliklerinden faydalanmaktadırlar. Virüslerden diğer bir farkı bir yazılımda ve işletim sisteminde açık bulduğunda yüzlerce ya da binlerce kopyasını yaparak gönderebilecekleri her yere gönderebilirler (SCTZine, 2016). Son olarak, solucanlar sisteme bulaşmadan önce sistemde kurulu Antivirüs ve Güvenlik Duvarı (Firewall) uygulamalarını kapatabilme mekanizmalarına sahiptir (Uslu, 2007). Canbek ve Sağıroğlu (2007) tarafından yapılan bir çalışmada ise solucanlar; e-posta, anında mesajlaşma (Instant Messaging), internet ve ağ solucanları olarak dört grupta listelenmiştir.

Solucanlar normalde hedef gözetmeksizin saldırı düzenleyebilirler. Fakat literatüre hedefli olarak saldırı düzenleyen Stuxnet solucanı, bir ilk olarak İran'ın Natanz kentinde bulunan uranyum zenginleştirme tesisine sızmıştır. Stuxnet isimli solucan taşınabilir bir bellek ile İran'da Natanz tesislerindeki bilgisayar sistemlerine bulaştırılmıştır. Akabinde bu solucan kendini kopyalamak vasıtasıyla çoğalmış ve bilgisayar sisteminin birçok ünitesine sızmıştır. Bu solucanın temel amacı PLC (Programmable Logic Controllers) kullanan ve gerçek zamanlı veri toplama, kontrol ve izleme yapan SCADA sistemlerini etkilemektir. Böylece etkilenen sistem hatalı çalışmaya başlamıştır. Ayrıca bir bilgisayarı ele geçiren bu solucan, yerel ağda paketleri dinleyerek ortadaki adam atağı düzenlemiştir. Bu yöntem ile

elde edilen ağ paketlerindeki PLC kodlarını değiştiren solucan sisteme hasar vermiştir (Shakarian, Shakarian ve Ruef, 2013; Holat, 2021).

3.1.3. Bilgisayar Virüsleri

Kötü yazılımlar kategorisine giren virüsler, eskiden beri bilinen bilgisayar veya bilgisayar ağ sistemlerine sinsi bir şekilde bulaşan ve kendilerini dosya içeriklerine saklayan, kullanıcıya ve bilgisayara zarar verme amaçlı çalışan küçük kapasiteli bilgisayar programlarıdır. Saldırganlar tarafından hazırlanan virüs içeren dosyalar birçok yolla sistemlere bulaşabilir. Bu yollar incelendiğinde ya e-posta yoluyla ya da USB sürücüler ve ya disketler gibi taşınabilir medya olduğu görülmektedir. "Brain" adlı ilk bilgisayar virüsünün 1986 yılında geliştirildiği bilinmektedir. Bilgisayar virüslerinin diğer kötücül yazılımlardan en önemli farkı insan etkileşimine gereksinim duymasıdır. Virüs içerikli dosya kesinlikle bir kullanıcı tarafından çalıştırılmalı ve yönetilmelidir. Bir virüslü dosya açıldığında, bir e-posta okunduğunda, bir sistem önyüklemesi veya virüs bulaşmış bir program çalıştırıldığında virüs gizlice yayılmaktadır (Peikari ve Fogie, 2002; Skoudis, 2003).

Bilgisayar virüsleri dört kategoride incelenmektedir (Canbek ve Sağıroğlu, 2007):

- Dosya virüsleri,
- Önyükleme (boot) virüsleri,
- Makro virüsler,
- Betik (script) virüsler

3.1.4. Truva Atı (Trojen)

Siber saldırganların en çok kullandığı kötü amaçlı yazılım türlerinden birisi Truva Atı (Trojen) saldırılarıdır. İsmini mitolojideki truva atından almaktadır. Bu saldırılar, yerel alan ağları (LAN - Local Area Network) ve kişisel bilgisayarlara sızmak için kullanılan yazılımlardır. Örnek olarak e-posta ile gelen bir kartpostal ya da ilgi çeken bir mesaj açıldığında farkına varılmadan bir truva atı cihaza yüklenebilmektedir (Marks, 2007). Truva atları genellikle siber kurbanların insanların, güvenilir bir kaynaktan geldiğini düşündükleri bir programı açmak vasıtasıyla yayılmaktadırlar (Baltazar, Costoya ve Flores, 2009).

Truva atlarının birden çok türü bulunmaktadır. Literatürde bunlar 5 türde ele alınmıştır. Sırasıyla bunları listelemek gerekirse; siber saldırganının siber kurban bilgisayarlara uzaktan iletişimini sağlayan *Uzaktan Erişen Truva Atları(UETA),* kayıtlı olan tüm şifreleri araştıran, bulan ve belirlenen e-posta adresine gönderen *Şifre Gönderen Truva Atları,* klavyeden basılan her tuşun kaydını tutan *Klavye Girişini Kaydeden Truva Atları,* dosyaları silen ya da tamamen yok eden *Zarar Veren Truva Atları*, bilgisayarınızın güvenliğini sağlamak için kurulan programları devre dışı bırakan *Program Denetim Yazılımlarını Kapatan Truva Atları* olarak karşımıza çıkmaktadır (Uslu, 2007; Kara, 2019).

3.1.5. Arka Kapı (Backdoor)

Arka Kapı (Backdoor), bilgisayar sistemlerinin güvenliğini veya şifrelemesini ekarte eden gizli bir yöntem olarak bilinmektedir. Bu sebepten dolayı bilgisayar sistemi yetkisiz erişim ve eylemlere karşı savunmasız kalmaktadır. Arka Kapı olarak adlandırılan zararlı yazılımlar da siber suçlular için arka kapı oluşturmayı hedefleyen zararlı türleridir. Böylelikle bu güvenlik açıklarından doğan arka kapılardan suçlular sızabilmektedir. Günümüzde Antivirüs programları sayesinde tespiti kolaylaşmıştır. Genellikle bilgisayar sistemlerinde oluşabilen güvenlik zafiyetlerinden yararlanmaktadırlar. Arka kapılar ile Truva atları zaman zaman karıştırılabilmektedir. Her iki yazılımda hedef sisteme sızmaya yarar fakat arka kapı, Truva atı gibi sistemde değişikliklere gitmez sadece sisteme erişimi olanaklı hale getiren gizli yapılardır (Canbek ve Sağıroğlu, 2007).

3.1.6. Casus Yazılımlar (Spyware)

Casus yazılımlar, internet üzerinde sistemlerin tarama geçmişini ve izlerini kayıt altına alabilen kullanıcı izni olmaksızın kendi kendini yükleyebilen gizlilik açısından çok tehlikeli yazılımlardır (Gustin, 2003). Bunun yanında bir başka ifadeyle casus yazılım, kullanıcıların önemli bilgilerinin ve yaptıkları işlemlerin, kullanıcının izni gerektirmeden toplanmasını ve bu toplanan bilgilerin kötü niyetli kişilere aktarılmasını amaç edinmiş yazılımlar olarak tanımlanabilmektedir. Bilgisayarlara veya sistemlere tuzak nitelikteki yazılımların kurdurulması ile bilgilerin aktarılması sağlanmaktadır (Canbek ve Sağıroğlu, 2007).

3.1.7. Reklam Yazılımları (Adware)

Reklam yazılımları İngilizce ismi "Adware" olan yazılımların temel özelliği arka planda çalışmalarıdır. Sistemlerin çalışma performansını ciddi şekilde düşürebilmektedirler. Temel amaçları arama isteklerini reklam sitelerine yönlendirmek, girilen web sitelerinin türleri hakkında bilgiler toplamaktır. Bunlar, paylaşılan ücretsiz yazılımlar ve virüs içeren web siteleri vasıtasıyla sistemlere bulaşmaktadırlar (Kaspersky, 2019). Diğer kötü yazılım türlerine göre daha az tehlikeli olduğu bilinmektedir.

3.1.8. Mantık Bombaları (Logic Bombs)

Mantık bombası, bir uygulamayı başlatmak veya belirli bir tarih / saate gelindiğinde olayın tetiklenmesini sağlayan ya da belirli bir olay olduktan sonra tetiklenmesi için gömülü kodlardan ibaret olan kötü amaçlı yazılımdır. Siber suçlular, mantık bombalarını çeşitli şekillerde kullanabilmektedir. Örneğin, 1982 yılında ABD, Sibirya gaz boru hattını izleyen ve kontrol eden bilgisayar sistemine bir bilgisayar kodu eklemiştir. Bu kod sayesinde sistemi denetleyen bilgisayarın yanlış çalışmasını sağlayarak, Sibirya gaz boru hattını patlatmıştır. Ayrıca, bir saldırıda da saldırganlar truva atı, keylogger ve mantık bombası birlikte saldırı geliştirebilmektedir.

3.1.9. Bukalemun (Chamelon)

Bukalemun yazılımları, sistem içerisinde normal bir program gibi çalışmaktadır. Bunlar yazılımlar iyi bir şekilde programlandırıldıklarında yasal yazılımların hareketlerini taklit etme yetenekleri vardır. Çalışma prensibi olarak sisteme giren yazılımlar, sistemin arka planında bir takım hile ve aldatmaya başvurmaktadırlar. Akabinde yazılım, çok kullanıcılı bilgisayar sistemlerinde kullanıcı hesap özelliklerini (ad ve şifre) taklit edip gizli bir dosyaya kaydetmektedir. Sonrasında kullanıcıya sistemin bakımda olduğunu ve belirli süre kapalı olacağını ifade eden bir uyarı mesajı göstermektedir. Bu sayede bukalemun programını yürüten saldırgan, bu bilgileri içeren dosyaya erişerek kullanıcıların adlarını ve şifrelerini içeren özel bilgileri ele geçirmektedir (Akbulut, 2017; Aslay, 2017; Geçmez, 2019; Gül, 2020).

3.1.10. Kök Kullanıcı Takımı (Rootkit)

Rootkit, siber saldırganların hedefteki bilgisayar veya sisteme erişmesini ve bu bilgisayarı kontrol etmesini sağlamak için tasarlanmış zararlı bir yazılımdır. Çoğu rootkit, bilgisayar yazılımlarını ve sistemde üzerinde çalışan işletim sistemlerini etkilemektedir. Ancak bazıları donanımını ve gömülü aygıt yazılımlarını da etkileyebilmektedir. Rootkit'ler sistemde gizlenmede uzmandırlar fakat gizli kaldıkları süre zarfında etkinliklerine devam edebilirler.

3.1.11. Mesaj Sağanağı (Spam,Junkmail)

E-posta yani başka bir deyişle email dünya genelinde mesaj alıp göndermek, mesaj okumak ve saklamak son olarak da randevularımızı planlamak amaçlı kullanılan en eski haberleşme yöntemi olarak bilinmektedir. Etkileşimli bir şekilde günden güne devamlı yaygınlığı artan bu iletişimin yöntemi üzerinden siber saldırganlar, virüs yazılımcıları ve dolandırıcılar, içeriği merak ve ilgi uyandıran eğlence, reklam, duygu sömürüsü, yardım ve bankacılık vb. ile ilgili gibi olan spam niteliğinde e-postalar göndermektedir. Zararlı kodlar içeren bu e-postalar kullanıcılara ait adres defteri, İnternet bankacılığı kimlik bilgileri, kullanıcı girişi yapılan siteler, mesajlaşma içeriği gibi önemli ve gizli bilgileri elde etmektedirler (Şahinaslan, 2007). Mesaj sağanakları, internet kullanıcılarının sıklıkla karşılaştıkları ve muzdarip oldukları zararlı yazılımların adeta başını çekmektedir (Canbek ve Sağıroğlu, 2007).

3.1.12. Tarayıcı Ele Geçirme-Soyma (Browser Hijacking)

Tarayıcı Soyma yöntemi, kullanıcının haberi ve bilgisi olmadan web tarayıcısının ayarları üzerinde oynama yapan bir saldırı olarak bilinmektedir. Eylemlerini genellikle web tarayıcısı eklentisi olarak ve başlangıç sayfası, varsayılan arama motoru ve yeni sekme sayfasını değiştirerek başlatırlar. Siber saldırganlar tarafından değiştirilen ve uyarlanan giriş sayfaları çoğunlukla arama motoru sayfalarıdır. Bu sayfalarda genellikle casus yazılımı görevi görmektedir. Böylelikle tarayıcı korsanları, arama terimlerini, ziyaret edilen sayfaları, yüklenilen dosyaları, IP bilgilerini ve girilen bilgileri kolaylıkla elde ederler. Bilgisayar

sistemlerine bulaştıktan sonra ciddi performans kayıplarına yol açan bu yöntemde, kullanıcıların web tarayıcılarının ana sayfa ve sık kullanılanlar listesi de sıklıkla değişmektedir (Adır, 2019).

3.1.13. Korunmasızlık Sömürücü (Exploit)

Bilgisayar sistemlerinde tespit edilen bir güvenlik zafiyetinin kullanımı anlamına gelen yöntem ve araçların tümüne exploit işlemi denmektedir (Özavcı,2013). Bu işlemin temel amacı güvenlik açığının riskini kolay bir şey şekilde göstermek ve çalışan bilgisayar sistemleri üzerinde gerçekliğinin doğrulanmasıdır. Exploit'lerde açık kaynak kodlu yazılımlar kullanılmaktadır. Açık kaynak kodlu olmanın avantajı test işleminde kötü niyetli kişiler tarafından oluşturulmuş zararlı kodların sisteme bulaşma durumu kontrol edebilmesidir. Piyasada hali hazırda bulunan ticari yazılımlar internet üzerinde yayınlanmış Exploit'leri kendi bilgisayar sistemlerine dâhil ederek tarama kütüphanelerinin kapsamını arttırmaktadır (Algaç, 2020).

3.1.14. Klavye Dinleme Sistemi (Keylogger)

Bilgisayar veya mobil cihaz kullanıcılarının klavyeden girdikleri bilgileri arka planda yakalayıp, saklayan ve bu bilgileri siber korsana yönlendiren casus yazılımlardır. Klavye dinleme yöntemi 1980'li yıllardan bu yana etkin ve etkili bir şekilde kullanılmaktadır. Zararlı ve casus yazılımlara karşı oluşturulan koruyucu programların çoğu, klavye dinleme yöntemini yeteri kadar önemsememektedirler. Bu nedenle kullanıcıların bu tür yöntemlere karşı önlem almaları ve koruyucu programları kullanmaları gereklidir (Canbek ve Sağıroğlu, 2007; Mohay vd., 2003).

3.1.15. Telefon Çevirici (Dialer)

Siber kurbanlara yüksek miktarda telefon faturası ödetmek amacı güden zararlı yazılımlardır (Koçoğlu,2019). Genelde kullanılan bağlantı numaralarını uluslararası uzak mesafe telefon numaraları ile değiştirerek bağlantı numarasını çeviren kişi farkına varmadan ödeyeceği miktar sürekli artmaktadır (Akbulut, 2017). Genellikle yüksek ücreti nedeniyle

900'lü hatlara yönlendirme yapan bu kötücül yazılımlar temelde iki çeşittir. Birincisinde aldatma ile kullanıcının bu programı internet üzerinden indirmesi sağlanır ve çalıştırılır. Diğerinde ise siber korsan, bilgisayara sızarak ve kullanıcı internete bağlandığı an bağlantıyı koparark istediği telefon numarasına yönlendirmektedir (Yazıcıoğlu, 2006).

3.1.16. Ekran Kaydedici Yazılımlar (Screenlogger)

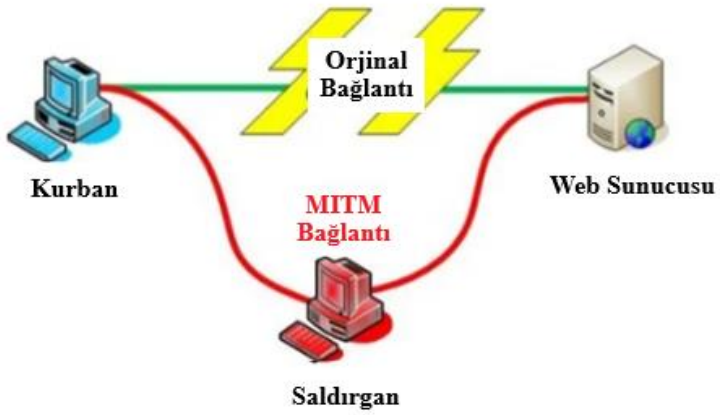
Bir başkasına ait kişisel bilgilerin yetkisiz kişiler tarafından kullanılması olarak bilinen kimlik hırsızlığı (identity theft) (Kocamaz, 2009) yönteminde çoğunlukla dolandırıcıların tercih ettiği yöntemlerden biri de Ekran kaydediciler (Screenlogger) yazılımlarıdır (Reis, Gülseçen ve Bayrakdar, 2010). Saldıranlar bir Truva atı yazılımı aracılığıyla tuş kaydedici programları sisteme yerleştirirler. Böylelikle herkes tarafından ortak kullanılan veya güvenilmeyen bir bilgisayara yerleştirilen bir ekran kaydedici program bilgisayar üzerinde yapılan bütün işlemleri öğrenebilir (Ergüç, 2008).

3.2. Kimlik Avı - Oltalama Saldırıları (Phishing)

Kimlik avı saldırıları olarak adlandırılmaktadırlar. Genellikle güvenli zannedilen kaynaklardan gönderilmiş e-postalar sayesinde özellikle tüzel kişilerin internet ağı üzerinde sitelere giriş bilgilerini, alışveriş için kaydettikleri ya da anlık kredi kartı bilgilerini izinsiz bir şekilde elde etmek amacı gütmektedir. İlk aşama olarak kurbana bir e-posta gönderilerek e-postadaki linke giriş yapılması başka bir tabirle linke tıklanması sağlanmaktadır. İkinci aşamada kurban linke tıkladığında saldırganların yönlendirdiği siteye gidilmektedir. Son aşama olarak kurban burada kendisine ait bilgi giriş alanlarını doldurulduğunda bu bilgiler artık saldırganlarla paylaşılmış olmaktadır. Örnek olarak bir bankadan kendisine e-posta geldiğini zanneden kurban, kredi kartı bilgileri ya da hesap bilgilerini yönlendirilen web sayfasında tekrar girerek bilgilerini güncellenmektedir. Fakat yönlendirilen sistem aslında saldırganlar tarafından üretilen web siteleridir. Bu durumda URL alanında bile banka sistemine yakın bir internet adresi görünmektedir. Kandırma ve yanıltma üstüne düzenlenen bu saldırılar özellikle internet ortamında yeni tanışmış ve bilgisayar açısından uzman olmayan kişileri hedef almaktadır.

3.3. Ortadaki Adam Saldırısı (Man in the Middle -MITM)

Ortadaki Adam Saldırısı (Man in the Middle -MITM), bir siber saldırganın bilgisayar ağından kullanıcılar arasındaki ya da bir kullanıcı ile bir web uygulaması arasındaki iletişimi gizli bir şekilde takip edip veri toplaması amacıyla yapılmaktadır. Kişisel veriler, şifreler ve bankacılık bilgilerini ele geçirmek için bilgisayar ağındaki bir kullanıcı ya da cihazı taklit eden bu saldırı türü önemli bilgiler olan oturum açma kimlik bilgilerinin değiştirilmesine ya da para transferi yapılmasına yol açarak ciddi hasarlar verebilir.



Şekil 3.1. Ortadaki Adam Atağı Yapısı

3.4. Servis Reddi Saldırıları (DoS-Denial of Service, DDoS-Distributed Denial of Service)

Tek bir kaynaktan yapılan hizmet dışı bırakma saldırısıdır. Bir hedefe saniyede binlerce paket gönderilerek sistemin cevap veremez duruma gelmesi hedeflenmektedir. Hedef sistem kapasitesi üzerindeki yüke cevap veremez ve servis dışı kalır. Sistemlerin erişilebilirliğini engellemeye yönelik saldırı türüdür. Zombi bilgisayar ağları olan botnetler ile gerçekleştirilebilen saldırıdır. Tespit edilmesi zor bir saldırı türüdür. Çünkü gözle görülür bir değişiklik yoktur. Ağ izleme uygulaması ya da Güvenlik Duvarı (Firewall) incelemelerinde fark edilebilir. Bir bilgisayar sistemi için kullanıcı sayısı, internet ve ağ

hattının kapasitesi, anlık istek sayısı gibi değerler önem arz etmektedir. Belirlenen değerlerin üzerindeki yükü sistem kaldıramamaktadır. DDoS ile saldırıyı yapan gizlenebildiğinden tespiti çok zordur. Çünkü siber saldırgan direkt olarak saldırıya dâhil olmaz. Yüksek seviyeli bir DDoS saldırısı, adeta karayolunda bir trafik sıkışıklığı gibidir ve düzenli trafiğin kesebilir. Fakat DDoS saldırıları, bazı durumlarda kapasite üstü istekle yapılmayabilir. İşletim sistemlerinde ve web sunucu uygulamasında oluşabilecek güvenlik zafiyetlerinden yararlanılarak sistem erişilemez hale getirilebilir. Bu saldırılar genellikle politik amaçlı ya da uluslararası kamu kurumlarına düzenlenen siber saldırılardır. Bu saldırılar siber savaşlarda etkin olarak kullanılmaktadır. En etkili DDoS atakları, mobil telefon, bilgisayar veya IOT cihazlarına bulaşan zararlı yazılımlar sayesinde gerçekleşir. En büyük DDoS saldırılarından biri de 2016 yılında Amerika'da ki DNS sunucularına yapılan saldırıdır. Bu saldırı sonucunda bir anda dünyadaki en büyük 85 web sitesi ortadan kalkmıştı. Bu saldırıda 1.2 terabitlik gibi yoğun istek gönderilmiştir (Yönak, 2017).

DDoS saldırıları, doğal olarak işleyen ağ hizmetine devamlı istek göndererek sistemin meşgul olmasını ve böylelikle bir süre sonra sistemin çalışmaz hale gelmesini sağlamaktadır. Bu açıdan DDoS saldırısı için, siber saldırganların kapasite üzeri sorgu göndermesi gereklidir. Bu bağlamda saldırganların birden çok cihaza ihtiyaçları bulunmaktadır. DDoS saldırılar genelde ele geçirilmiş bilgisayar, akıllı telefonlar, cihazlar ve internete bağlanabilen diğer cihazlardan oluşan adeta bir ordu gibi çalışmaktadır. Bu ordu içinde beraber çalışan cihazlar botnet denilen yapılar oluşturmaktadır.

3.5. Kimlik Bilgisi Doldurma Saldırıları (Credential Stuffing Saldırıları)

Bu saldırı kapsamında, bir siber saldırganın bir güvenlik açığı sonucunda elde edilmiş verileri kullanarak, sahip olduğu kayıt verilerini otomatik olarak numaralandırarak bir platformdaki kullanıcı hesaplarına erişim sağlamaya çalıştığı siber saldırılardır. Bu türdeki bir saldırıda öncelikle siber saldırganın kullanıcı kimlik bilgileriyle bir veri tabanına yasal veya yasal olmayan bir yoldan sahip olması gerekmektedir. Sonrasında eldeki kimlik bilgileriyle savunmasız durumda olan platforma bağlanmalıdır. Çünkü mevcut bilgilerinin doğruluğu her zaman kesin değildir, siber suçlunun stratejisi ise kimlik bilgileri eşlenene

kadar bu bilgileri yineleyerek otomatik olarak yetkilendirme sürecini başlatmaktır. Ayrıca yetkilendirme işlemleri, bu platformun onları gerçek kullanıcı olarak görmesi için özel botnetler kullanılarak gerçekleştirilmektedir. Sonunda giriş başarılı bir şekilde gerçekleşirse, saldırı da başarılı olmuş demektir (Şimsek, 2021).

3.6. Şifre Saldırıları (Password Attack)

Temel amacı kullanıcı tarafından sisteme girilen şifrenin kırılmasıdır. Günümüz sistemlerinde giriş için kimlik ve yetki denetimi sebebiyle kullanıcı adı ve şifre gereklidir. Özellikle bir hesap üzerine saldırı düzenlenirken, kullanıcı adı ve e-posta bilgilerin bilinmektedir. Buna istinaden bu hesabın şifrenin kırılmaya çalışılmaktadır. Bununla birlikte şifre içeren; .rar, .zip, .docx vs. uzantılı dosyaları açmak içinde bu yöntem kullanılmaktadır. Bu nitelikteki saldırılara karşı daha karmaşık ve çözülmesi zor güvenli şifreler kullanılmalıdır. Yoğunlukla güvenlik açığı oluşturan zayıf şifreler şöyledir:

Çizge 3.1. Zayıf Şifre Örnekleri (Bolubeyi, 2013)

Campus	**Business**	**Residence**
123456	**123456**	**123456**
password	**password**	**password**
12345	**test**	**test**
admin	**test123**	**123**
1234	asutcmhack123@	**1234**
123	passwd	**test123**
root	40232046bad	passwd
qwerty	!@# asutcmhack!@#	1
abc123	**root**	12
administrator	**12345**	**root**
12345678	**qwerty**	**admin**
user	**1234**	changeme
linux	mysql	abc123
test123	**123**	**qwerty**
guest	apache	**guest**
mysql	master	1q2w3e
1234567	**user**	**user**
apache	linux	newpass
master	**guest**	asdfgh

3.6.1. Kaba Kuvvet Saldırısı (Brute Force Attack)

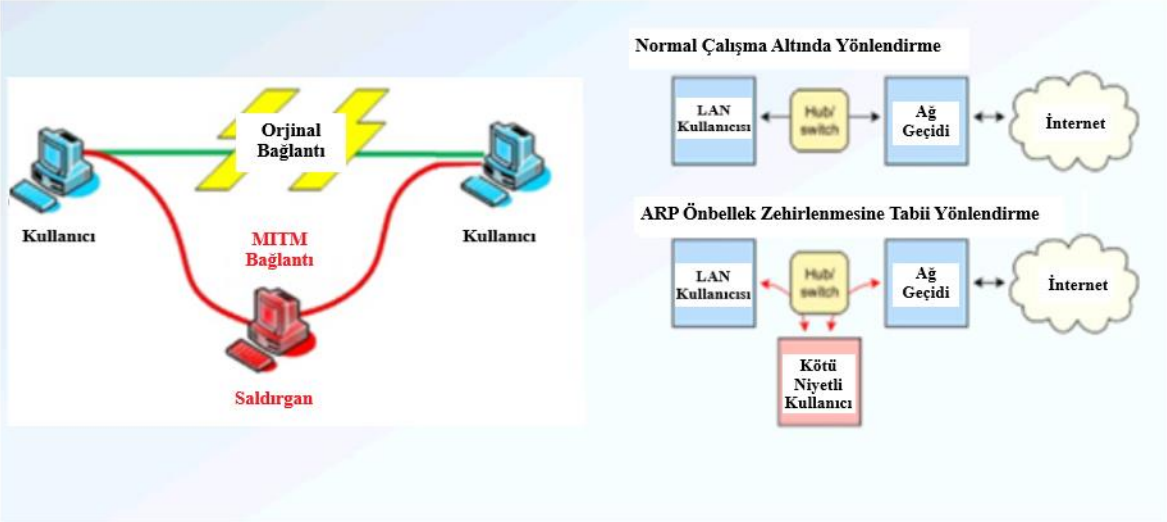
Kaba kuvvet saldırıları, şifrenin elde edilebilmesi için tüm ihtimallerin denenmesi mantığına dayanmaktadır. Bu saldırı türünde harfler, sayılar, özel karakterler kullanılarak değişken uzunlukta tüm şifre ihtimalleri denenmektedir. Bu kırma işlemi elde edilmek istenen şifrenin gücü ve karmaşıklığı, şifre kırma süresine etki etmektedir. Teoride yeteri kadar süre ve kaynak var ise elde edilemeyecek şifre bulunmamaktadır. Kaba kuvvet saldırısı yapan programlara internetten ulaşılabilmektedir.

3.6.2. Sözcük Tabanlı Saldırılar (Dictionary-Based Attack)

Sözlük tabanlı saldırılar, milyonlarca sayıdan ve kelimelerden oluşan listeler vasıtasıyla yapılmaktadır. Kaba kuvvet saldırısına benzemektedir. Fakat bu yöntemde, ihtimal ve tahminler yerine siber saldırganın sahip olduğu kelime listesi üzerinden şifreler tek tek denenmektedir. Şifre, siber saldırganın listesinde bulunuyorsa, şifre kırılır. CWWordListMaker gibi programlar liste oluşturmada kullanılmaktadır.

3.7. ARP Spoofing

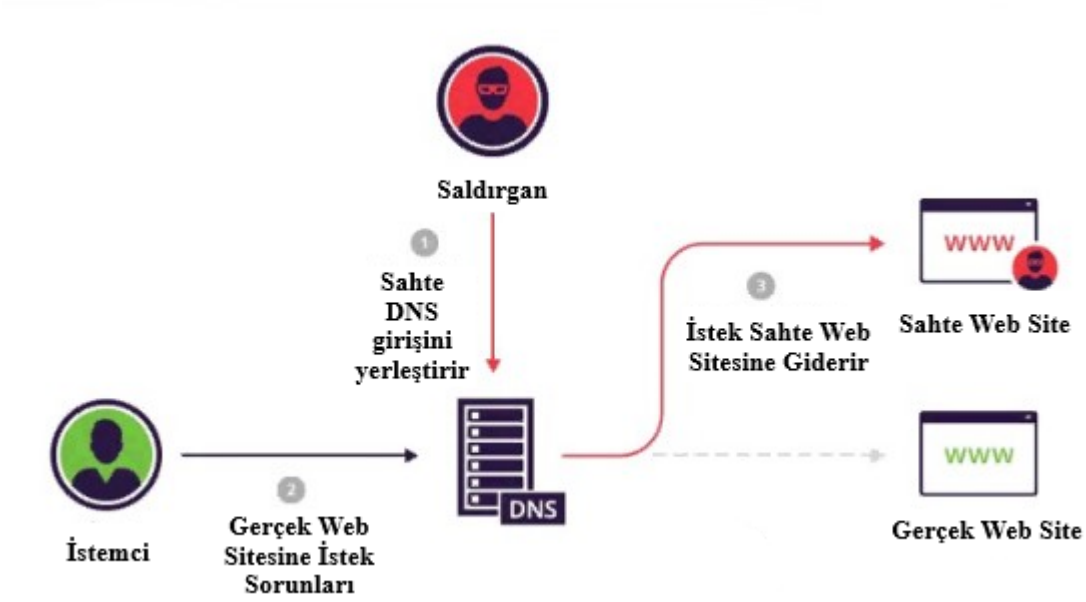
MAC ve IP adresi tabloları istismar edilerek hedef bilgisayardaki ağ trafiğinin dinlenmesi ya da değiştirilmesi için yapılan bir saldırı türüdür. Bu saldırının başarılı bir şekilde gerçekleşmesi için saldırgan kullandığı cihazın MAC adresini hedefteki bilgisayarın ARP tablosuna “Ağ Cihazı MAC Adresi” olarak ve ağ cihazı ARP tablosuna ise “Hedef Bilgisayar MAC Adresi” olarak eklemelidir. Böylelikle araya girerek ağ trafiğini dinler ya da değiştirebilmektedir.



Şekil 3.2. ARP Spoofing Saldırı Örneği (Sancar, 2019)

3.8. DNS Spoofing

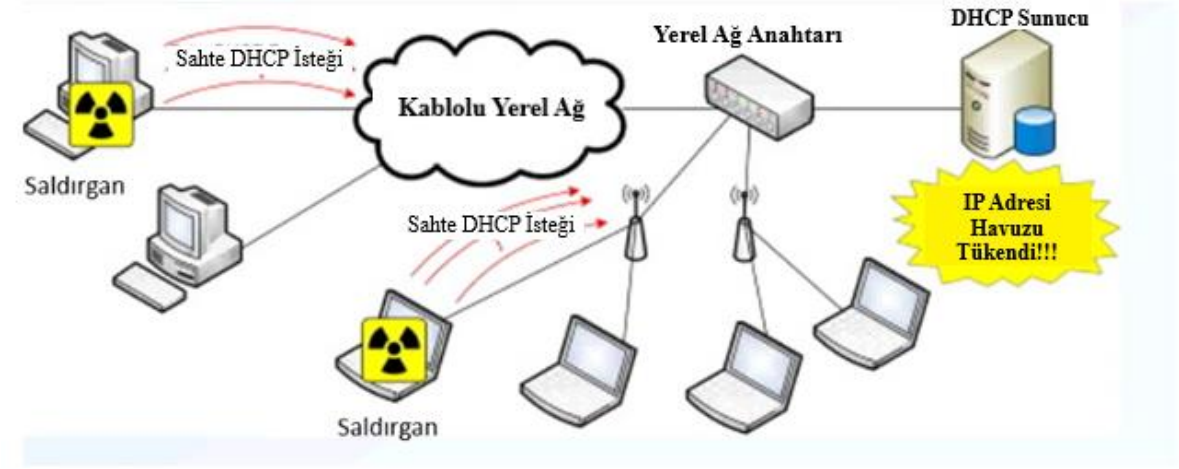
Bu saldırı yönteminde bir DNS sunucusunun ön bellek veri tabanında bulunan veriler değiştirilerek ya da yeni veriler eklenerek DNS'in hatalı IP adres eşleşmesi ve veri trafiğinin bir başka bilgisayara yönlenmesini sağlanmaktadır. Böylelikle bir siber saldırgan tüm DNS isteklerini ve ağ trafiğini kendi makinesine yönlendirebilir, kötü bir şekilde istismar edebilir ve verileri elde edebilir. Bu saldırı türünün tespit edilmesi çok zor olduğundan tehlikeli saldırılardan biridir. Saldırgan kişi bu saldırıyı dışarıdan yapamaz. Mutlaka iç ağa erişmesi gerekmektedir. Kali Linux Ettercap ile yapılır.



Şekil 3.3. DNS Spoofing Saldırı Örneği (Kandemir, 2019)

3.9. DHCP Starvation

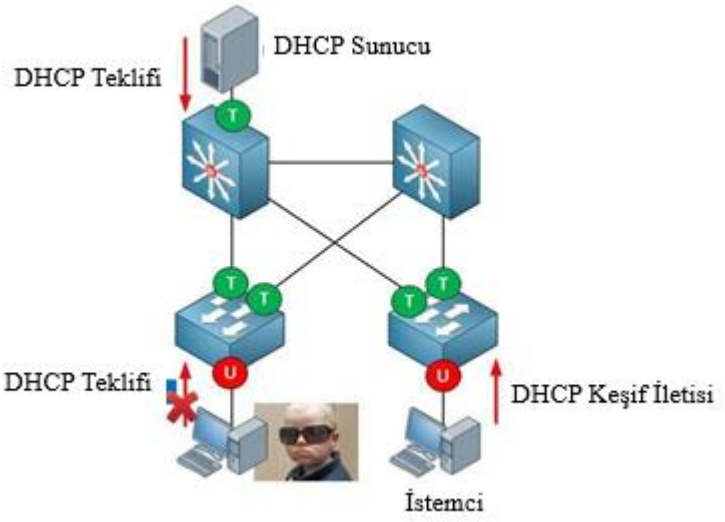
DHCP açlığı saldırısı olarak bilinmektedir. DHCP sunucularının hedefleyen hizmet dışı bırakma saldırısıdır. Saldırgan kişi sahte MAC adresleri ile DHCP'den çok sayıda IP talep eder. Ağdaki IP dağıtımından sorumlu DHCP sunucusu tüm bu sahte IP taleplerine cevap vermeye başlar. DHCP havuzundaki mevcut IP adresleri çok kısa sürede tükenir. Havuzdaki boş IP'ler tükenince gerçek ihtiyacı olan cihazlar IP adresi alamazlar. Bu sebeple kullanıcı mağduriyeti yaşanır. Bilgi Güvenliğinin erişilebilirlik ilkesi hedef alınıp, ihlal edilmiş olunur. IP adresi tükenince saldırganlar sahte bir DHCP sunucusu kurabilir ve yeni IP taleplerine bu sahte DHCP sunucusu üzerinden yanıt verebilir. Saldırgan böylece istediği gibi ağ cihazı belirler istediği alt ağı (subnet) oluşturur ve istediği ağ trafiğini de kendisi üzerinden de geçirebilir.



Şekil 3.4. DHCP Starvation Saldırı Örneği (Mukhtar, Salah, & Iraqi, 2012)

3.10. DHCP Spoofing

Saldırgan sahte bir DHCP sunucusu kurar. Sahte DHCP sunucu, ağa dâhil olmak isteyen istemcilerin DHCP Disco veri paketlerine DHCP Offer paketleri ile geri dönüş sağlar. DHCP Offer paketi, kullanıcıya gönderilen ağ bilgilerinde gateway kısmında saldırganın IP adresi yer alacak şekilde düzenlenir. Kullanıcı ise bu bilgilerin uygunluğunu belirten DHCP Request paketi döner. Son adımda ise DHCP Acknowledgement ile siber saldırganın yürüttüğü şekilde işlem tamamlanmaktadır. Artık kullanıcı bilgisayarında kayıtlı bulunan gateway adresi saldırganının belirlemiş olduğu adrestir. Bu andan itibaren kullanıcının ağ trafiği istenildiği gibi istismar edilebilir. Siber saldırganın oluşturduğu sahte bir siteye yönlendirilebilir ve trafiği saldırganın istenildiği gibi kullanılabilir. Bu saldırı en tehlikeli saldırı türleri arasında yer alır.



Şekil 3.5. DHCP Spoofing Saldırı Örneği (Yegin, 2015)

3.11. Sosyal Mühendislik Saldırıları

Bu saldırı türünde kullanıcı eylemlerindeki yanlışlar veya zaaflar kötüye kullanarak bir bilgisayar ya da ağ sisteminin ele geçirilmesi amaçlanmaktadır. Bir nevi "insan aldatma sanatı" olarak da bilinmektedir. İnternet tarihinin görülmüş en eski saldırı türlerinden biri olarak nitelendirilen sosyal mühendislik saldırıları için en önemli isim Kevin Mitnick olarak bilinmektedir. İnsan doğası gereği her zaman ve her yerde çeşitli hatalara düşebilmektedir. Bu açıdan siber saldırganlar sosyal mühendislik saldırıları ile sistemler gizli bir şekilde erişim yapabilmektedir. Bu yöntemsel saldırılarda genellikle oltalama, sahte aramalar, ters toplum mühendisliği, çöp karıştırma ve bilgi çalmak gibi birden fazla yöntem kullanılmaktadır. Bu teknikler hem tek bir kullanıcıya hem de bir kurum içindeki çalışanlarının bütününe de uygulanabilmektedir (Mitnick, 2006).

BÖLÜM 4

SİBER SALDIRILARDAN KORUNMA YÖNTEMLERİ

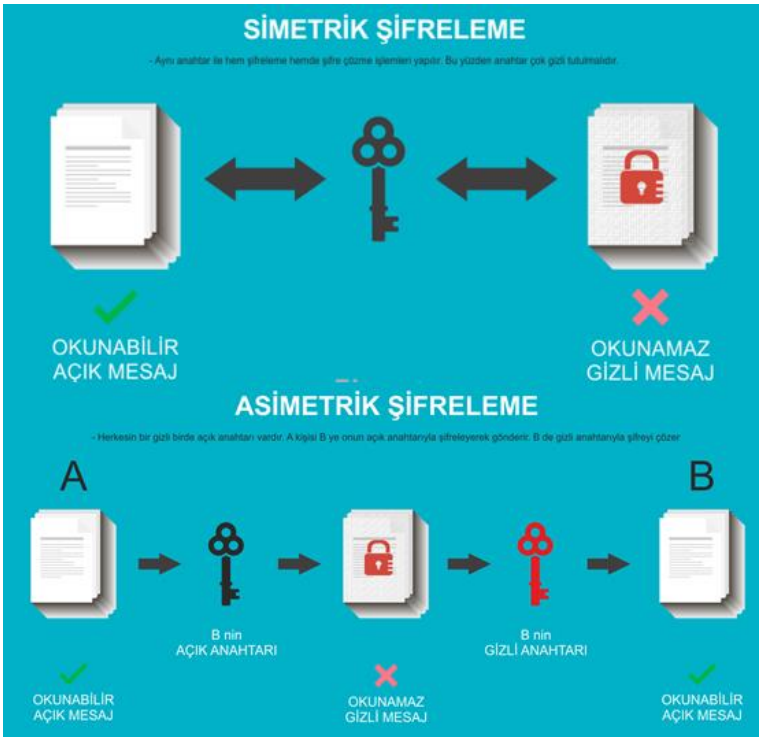
Son yıllardaki siber silah kullanım amaç ve kullanım alanları yaygınlaşmaktadır. Siber casusluk ve kimlik hırsızlığı hackerlar (bilgisayar korsanı) tarafından bilgisayarlarımızı sızılıp çalınma olasılığı yüksektir. Finans verileri hedef alan hackerlar internet kullanıcılarını tedirgin etmektedir. Siber saldırılara karşı alınabilecek korunma yöntemleri gelişen teknolojiye göre zamanla geliştirilip, yeni yöntemler geliştirilmektedir. Siber saldırılardan korunma için kullanılan yöntemlerden bazıları aşağıda açıklanmıştır.

4.1. Şifreleme

Şifreleme; veri, bilgi veya öz bilginin şifre ile korunması, saklanması veya istenmeyen kişilerin anlamasını zor kılma veya şifrelenmiş veri, bilgi veya öz bilgilerin çözülmesi üzerinde çalışan bir bilim dalı olarak bilinmektedir. II. Dünya Savaşında şifreleme yaklaşımları çok önemli rol oynayarak şifreleme bilimine ilgi artmıştır. Böylece yeni şifreleme yaklaşımlar geliştirilip, ABD tarafından laboratuvarlar kurulmuştur. II. Dünya savaşıyla birlikte devlet güvenliği sağlama amacıyla kriptografik standartlar geliştirilmeye başlanmıştır. Siber güvenlik sayesinde internet ortamı üzerindeki veriler, mobil ve sabit telefonlar, bilgisayarlar, televizyon, araba, uçak, ev aletleri, beyaz eşya, gemiler, uydu vb. gibi ortamlar üzerinde koruma sağlanmaktadır. Verilerin güvenli bir ortamdan diğerine aktarılıp, saklanmasında şifreleme bilimi kullanılmaktadır. Veriler, üçüncü şahıslar tarafından algılanmayacak ve öğrenilmeyecek şekilde farklı bir forma veriyi dönüştürme işlemi yapılmaktadır (Sağıroğlu & Alkan, 2018). Şifrelenen veriler siber alandaki doğru kişiler tarafından bilenen bir anahtarla deşifre edilip, okunabilmektedir.

Şifreleme sistemleri günümüzde iki temel çalışma alanına ayrılmıştır;

- Simetrik Şifreleme; bu yönteminde kullanılan algoritmalar hem şifreleme hem de şifre çözme için aynı anahtar kullanılmaktadır. Anahtarlar rastgele seçilip uzunlukları 128 ya da 256 bit olarak belirlenmiştir.
- Asimetrik Şifreleme; bu yönteminde kullanılan algoritmalar şifreleme için kullanılan anahtar açık anahtar olarak bilinip ve başka kişilerle rahatça paylaşılabilirken, şifre çözme için kullanılan anahtar özel anahtar olup gizli tutulması gerekmektedir. Bu yöntemde açık ve gizli kullanılan iki anahtar arasında matematiksel bir modül bulunur(Sağıroğlu & Alkan, 2018).



Şekil 4.1. Şifreleme Yöntemleri (Balat, 2018)

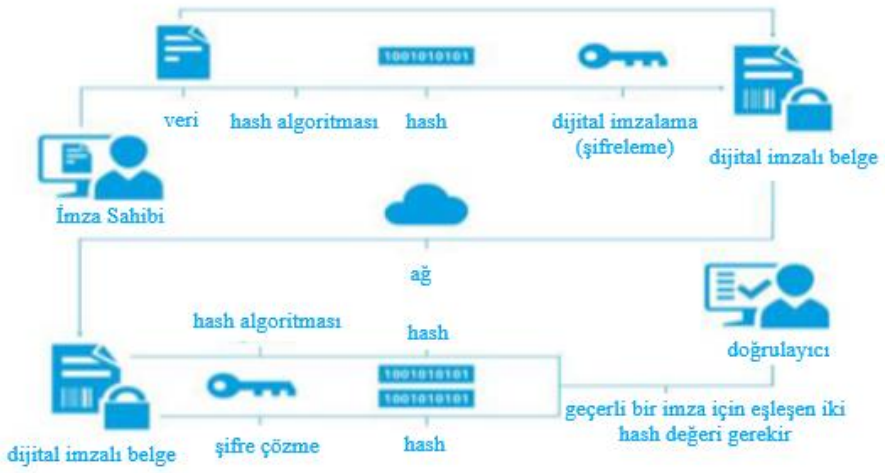
4.2. Sayısal İmza

İleri gelişmiş teknolojiler yardımı ile elektronik ortamda yaratılan, yollanan veya kabul edilen bilgilerin, bunları ileten kişi veya kurum ya da kuruluşa ait olduğunun

onaylanması için kullanılan bir haberleşme yöntemidir. Bu yöntem sayesinde verilerin kimden geldiği, mesajı alanların kim olduğu tescil edilmektedir. Aynı zamanda içeriğin değiştirilmemesi, başkaları tarafından ele geçirilse dahi anlaşılamaması en önemli amaçlardandır. Yapısında bit katarları bulunmaktadır. Bir elektronik imzanın temel nitelikleri şöyledir:

- Güvenilirlik,
- Taklit edilememek,
- Tekrar kullanılamamak,
- İnkâr edilememesi
- İçeriğe müdahale edememek,
- Yardımsız bir şekilde kullanılabilirlik,

şeklinde sıralayabiliriz. Dünyada ve Türkiye'de e-imza veya sayısal imza, elektronik ticaret, bankacılık, özel, kamu vb. birçok alanda kullanılmaya başlanmıştır. E-imza yaygınlaşarak devletin vatandaşlarıyla ilişkilerini elektronik ortama taşıyarak güvenli bir iletişim kanalı oluşturmaktadır (Sağıroğlu & Alkan, 2018).



Şekil 4.2. Sayısal İmza (Özdemir, 2020)

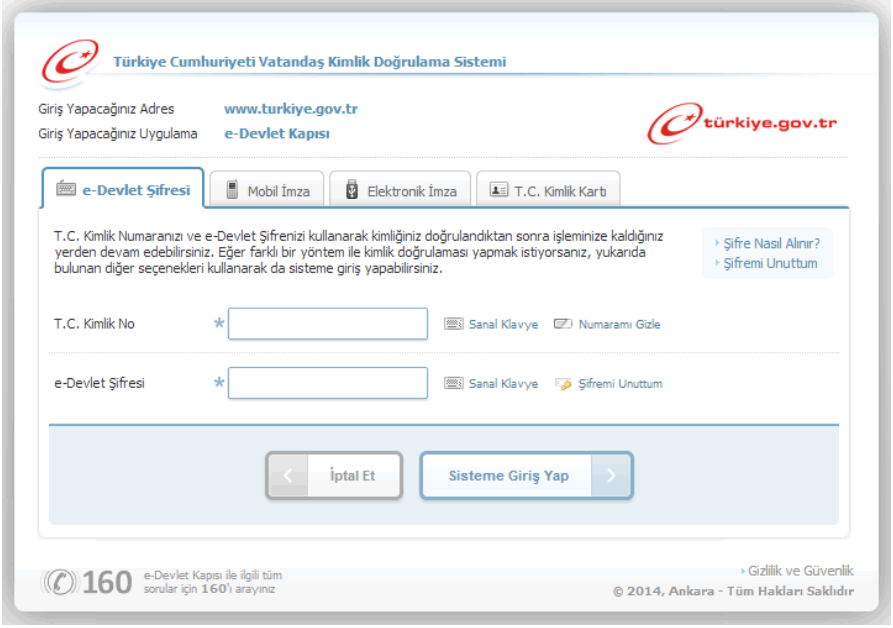
4.3. Steganografi

Steganografi, eski zamanlardan beri bilinen ve içerisinde gizli bilgiler ve mesajlar bulunan bilgileri ve içerikleri alıcısından başka birinin fark edemeyeceği şekilde gönderme sanatı olarak ifade edilmektedir. Steganografi kelime kökeni olarak Yunan alfabesinden türeyip dilimize geçmiştir ve anlam olarak örtülü yazı manasına gelmektedir. (Cummins vd., 2022) Bu yöntem ile gönderilmek veya aktarılmak istenen mesajla bir başka güvenli sayılan ortamda saklanmak vasıtasıyla üçüncü kişilerin bu mesajın farkına varmamaları amaçlanmaktadır. Steganografi asıl amaç gizli mesajın varlığını gizlemektir. Steganografi ile ulaştırılmak istenen mesaj bir başka bilinmeyen ortamda gizli bir biçimde tutularak, üçüncü şahısların bu iletilen mesajın mevcudiyetinden haberi olması engellenmektedir. Steganografi iletilmek istenen veriler, resim, ses, metin veya daha farklı formattaki dosyalar ile alıcısına ulaştırılabilmektedir. Tarihe bakıldığında Steganografi yönteminin hem şifreleme öncesi hem de sonraki dönemlerde kullanıldığı görülmektedir. Stenografi yönteminin özellikle hu dönemlerde ilgi çekmeme avantajından dolayı kullanıldığı düşünülmektedir. Steganografi yöntemi ile gizli bir iletişim kurulmaktadır. İki kişi arasında gerçekleşen bir iletişimi bir diğer kişinin fark edememesi söz konusudur. Bilimsel ortamda Steganografi ile ilgili yapılan alan çalışmaları 1984 yılında Simmons tarafından "Prisoner Problem" in tanımlanması ile ortaya çıkmıştır. Bu problemde Alice ve Bob hapishanededir ve hapishaneden kaçmak için planlar yapmaktadırlar. Fakat bu planların gardiyan Willie'ye fark ettirilmeden yapılması gerekmektedir. Eğer Willie bunu fark ederse kaçma planları suya düşecektir. Bu nedenle de çeşitli gizli haberleşme yöntemleri geliştirilmesi gerektiği ifade edilmiştir (Simmons, 1984).

4.4. Kimlik Doğrulama

Son yıllardaki veri sızıntıları çoğunda, ele geçirilmiş kullanıcı giriş bilgileri büyük rol almaktadır. Sadece tek bir kullanıcı/parola ile bağlanılan sistemler o parolanın açığa çıktığı ve ele geçirdiği zaman kadardır. Gelişen tehditler, tek bir parola bariyerini çoğu zaman geçebilecek haline geldiği için ikinci hatta üçüncü bir kimlik doğrulaması yapılma zorunluluğunu getirmiştir. Bağlanılacak sisteme ya da programa girerken parolanın yanında

tek seferlik kodlar veya biyometrik doğrulama işleminin yapılması sistemimizi siber saldırılardan korumak için iyi yöntemlerden birisidir.



Şekil 4.3. Kimlik Doğrulama (Edevlet, 2022)

4.5. Firewall (Ağ Güvenlik Duvarı)

Firewall, diğer ismi ile ağ güvenlik duvarı kurumun ağı ve diğer dışarıdaki ağlar arasında geçit görevi gören bir sistemdir. Özellikle internet erişiminde karşılaşılabilecek problemleri çözmek üzere tasarlanmış bir sistemdir. Ağın dışından ağın içine erişimin denetlenmesi burada yapılmaktadır. Bu sebeple erişim politikaları ile paraleldir. Güvenlik duvarları sadece dış saldırılara karşı sistemi korumakla kalmamakta ayrıca, performans arttırıcı ve izin politikası uygulayıcı amaçlar için de kullanılmaktadır. Bu çözümler yazılım veya donanımla yazılımın bütünleşmesi şeklinde olabilmektedir. Güvenlik duvarlarının grafiksel arabirimleri kullanılarak kurumun politikasına uygun bir şekilde erişim kuralları tanımlanabilmektedir. Güvenlik duvarı aşağıda belirtilen hizmetlerle birlikte çalışarak ağ güvenliğini sağlayabilmektedir (Karaarslan, 2003).

Proxy: “Vekil sunucu” ya da “ara sunucu” olarak bilinen proxy, bağlanmak istediğimiz bir web uygulamasında araya giren ve bağlantıyı istemci (client) için kendisi gerçekleştiren bir hizmettir. Proxy’nin kullanımı, uygulama temelli (application-level) güvenlik duvarı olarak da adlandırılabilir. Bu tür bir uygulama aynı zamanda kimlerin bu hizmetleri kullanacağını belirlemek ve performans amaçlı olarak hızlı bağlantı olanağı sağlamak için de kullanılmaktadır.

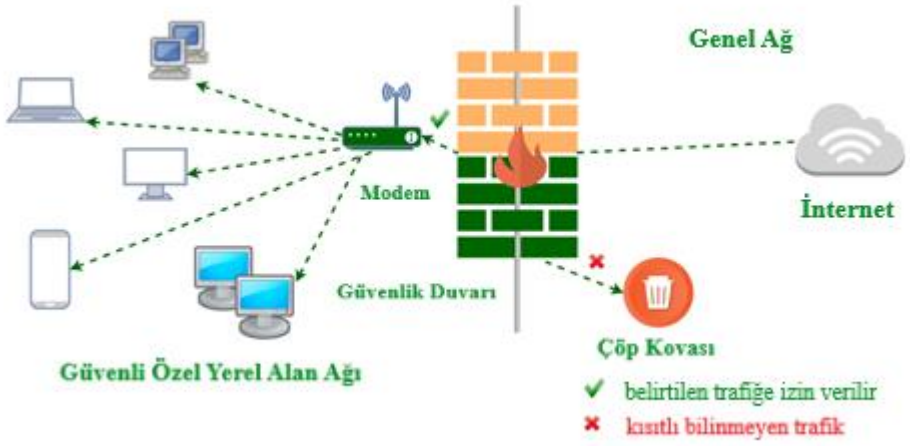
Antivirüs Çözümleri: Belirli işlevleri gerçekleştirmek için kullanılan HTTP, FTP ve SMTP protokollerinin trafiğini üzerinden geçirilerek virüs tarama işlemini yapmayı ve kullanıcıya gelmeden önce virüslerden temizlemeyi hedefleyen sistemlerdir.

İçerik Süzme (content filtering): Çeşitli yazılım ya da donanımlarla ulaşılmak istenen web sayfalarını, gelen e-posta’ları süzmeye yarayan sistemlerdir. Genellikle şirketlerde internet güvenlik duvarlarının bir parçası olarak content filtering kullanılmaktadır. Bu yöntem şirket çalışanlarının şirketin bilgi sistemi dışında herhangi bir sosyal medya platformuna erişiminin filtrelenmesi ve engellenmesinde kullanılmaktadır.

Özel Sanal Ağlar (Virtual Private Network-VPN): Şirketlerin şubeleri arasındaki iletişimi şifreleyerek güvenli iletişim sağlaması amaçlanmaktadır. Ortak kullanıma açık veri ağları (public data network) üzerinden kurum ağına bağlantıların daha güvenilir olması için VPN kullanılmaktadır. İletilen bilgilerin şifrelenerek gönderilmesi ve Genel / Özel (Public / Private) anahtar kullanımı ile verilerin başka kişilerce ele geçirilmesi önlenmektedir. Siber alanlarda VPN kullanan kurum ve kuruluşlar arttıkça bu alanda geliştirilecek politika adımları önem arz etmektedir.

Firewall’ın bilgisayarı tehditlerden ve saldırılardan koruyan bir donanım olduğu düşünülmektedir. Bu sayede hem internette güvenli kalınmakta hem de sadece ihtiyacı olan kişilerin yerel ağda ilgili yerlere erişimi sağlanmaktadır. Siber saldırılardan korunma yöntemi olarak Firewall kullanılmaktadır. Siber alanda yer alan veriler, bilgisayarlar, sunucular ve yönlendiriciler arasında gidip gelmektedir. Güvenlik duvarı ise bu akan veriyi denetleyerek güvenli olup olmadığını tespit etmektedir. Güvenli olmayan verilere karşıda bilgisayar ve sistemleri korumaktadır. Güvenlik duvarı, bilgisayarımızın uzaktan erişim ile bir başkası

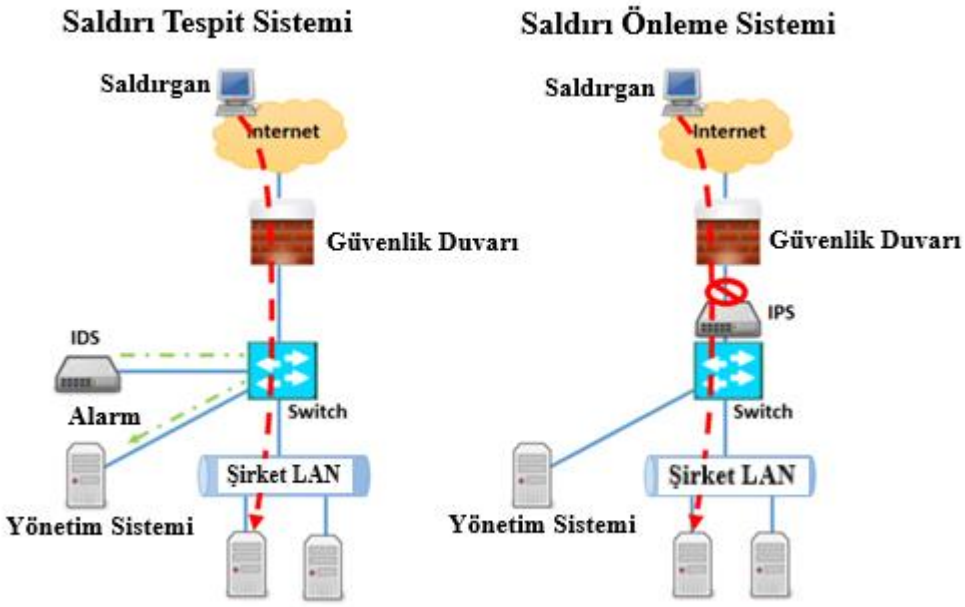
tarafından kontrol edilmesini engeller. Bu nedenle güvenlik duvarının ayarlarından casus yazılım ve uygunsuz içerikleri engelleyerek bilgisayarımızı siber saldırılardan korunabilmektedir.



Şekil 4.4. Firewall (Ayvaz, 2022)

4.6. Saldırı Tespit ve Engelleme Sistemleri (IDS/IPS)

Herhangi bir saldırının varlığı açısından bilgisayar ağında gerçekleşen faaliyetlerin takip edilmesi, tehdit ve ihlallerin tespit edilmesi için veri trafiğinin incelenmesi ve analizini sağlayan sistemlerin bütünüdür. Siber atakları engelleme sistemleri saldırıların saptar ve önlenmesi için gerekli güvenlik işlemlerini yapar. Bilgisayar ağlarının karmaşık olması, diğer ağların birçok erişim noktasına bağlı olması, siber saldırıların çeşitlenmesi, şifreleme ve güvenlik duvarlarının koruyamadığı göz önüne alındığında böyle bir sistemin geliştirilmesini kaçınılmaz kılmıştır. Bu sistemler, bilgisayar ağını belirli periyotlarda izleyerek gelişebilecek tehditleri belirler ve bu tehditlerle ile ilgili olay kayıtlarını (logları) tutmaktadırlar. Ayrıca siber saldırıları engellemek ve güvenlik uzmanlarına raporlamak gibi işlevlere de sahiptirler. Fakat bu sistemler bazı durumlarda tam tersi olarak kurumların güvenlik politikalarındaki açıkların ortaya çıkarılması amaçlı da kullanılabilmektedir.



Şekil 4.5. IDS/IPS (Güden, 2019)

4.7. Antivirüs

Bilgisayar, tablet, telefon gibi bilişim tabanlı teknolojilerde güvenliğini sağlamak amacıyla geliştirilen yazılım türüdür. Antivirüs yazılımları virüslere karşı bilgisayarı taramak, virüsten temizlemek, virüslü dosyaları kurtarmak ve virüse karşı koruma gibi birçok işlevi yerine getirmektedir. Bilgisayar, tablet, telefon, vb. internet bağlantısı aracılığıyla virüs tehditlerine açık hale gelmektedir. Bununla birlikte USB'ler, harici hard diskler ve SD kartlar gibi bilgisayara haricen bağlanan cihazlardan gelen virüslere maruz kalabiliriz.

Virüsler bilişim tabanlı teknolojilere sızarak verilerimizi ele geçirme, cihazın doğru çalışmasını engelleme, zararlı etkinliklerde bulunma gibi birçok olumsuz durumlara yol açabilir. Bu açıdan her bilgisayarın mutlaka lisanslı ve güncel bir antivirüs programı kullanması gerekmektedir.

Antivirüs programlarının çalışma prensibi; kötü amaçlı bir yazılımla ilk karşılaştığında ilk olarak kullanıcıya bir mesaj iletir ve ardından virüs içerdiğini düşünüyorsa yazılımla karantinaya alır. Bu karantina ardından çoğunlukla siler. Ancak bazı durumlarda

kullanıcıdan silme onayı alır. Bu programlar uzman siber güvenlik firmaları tarafından piyasa sürülür (Turknetblog, 2022).

BÖLÜM 5

SİBER SALDIRI ÖRNEKLERİ

Dünya üzerinde günden güne siber tehditler ve saldırılar artmaya devam etmektedir. Özellikle siyasi veya ekonomik amaçlar için casusluk ve sabotaj amacıyla ulaşım, enerji, iletişim gibi kritik altyapılara yönelik tehdit ve saldırılar önem arz etmektedir. Çünkü bu saldırılar yüzünden ülkeler ve barındırdıkları şirketler hem ekonomik hem de fiziksel açıdan ciddi hasarlar alabilmektedir. Bu bağlamda tezin bu bölümünde Dünya ve Türkiye'de yürütülmüş ciddi anlamda hasarlar veren siber saldırı örnekleri ele alınacaktır.

5.1. Dünya Genelinde Siber Saldırı Örnekleri

Burada tarihsel olarak sıralanmış şekilde 30 adet siber saldırı örneğine yer verilmiştir. Siber saldırıların hangi amaçla yapıldığı, nereye yapıldığı ve hangi yöntem ile yapıldığı verilmiştir.

5.1.1. Sibirya Siber Saldırısı (Logic Bomb)

İnternet tarihinde ilk siber saldırı olarak Sibirya'da 1982'de yaşanan patlama gösterilmektedir. Rus korsanlar, Kanada menşeli bir şirketten doğal gaz boru hatlarını kontrol etmek için kullandığı ve CIA tarafından yerleştirilen tuzak kodlar içeren virüslü bir yazılımı çalarak tesisteki bilgisayar sistemine eklemişlerdir. Bu olay sonunda Sibirya doğal gaz boru hattında bir mantık bombası niteliğinde yürütülen saldırı nedeniyle büyük bir patlama olmuştur.

5.1.2. Ay Işığı Labirenti (Moonlight Moze)

1998'de ABD'nin Pentagon, NASA, ABD Enerji Bakanlığı ve üniversitelere ait araştırma ve geliştirme sırları, askeri tesislerin haritaları, askeri yapılandırmaları ve askeri donanım tasarımlarını içeren birçok gizli bilgi "Moonlight Moze" olarak bilinen operasyon ile çalınmıştır. Yaklaşık yüz milyon dolar değerinde verinin ele geçirildiği ve bu bilgilerin Moskova'ya gönderildiği anlaşılmıştır.

5.1.3. Melisa

1999 yılında David L. Smith isimli yazılımcı tarafından tasarlanan ve Floridalı egzotik dansçının adının verildiği virüs olan Melisa virüsü, 26 Mart 1999 tarihinden itibaren e-postalar aracılığıyla yayılmaya başlamıştır. Virüsü içeren e-postada bir word dosyası bulunmaktadır. Gönderilen e-postanın ilgi çekmesi amacıyla "Erotik içerikli sitelerin" adreslerin adresleri yazılmıştır. Bu amaçla word dosyasını açanların bilgisayarlarına virüs bulaşmıştır. Virüs bilgisayar sistemindeki önemli dosyaları silmiş ve bilgisayar sistemine ağır hasarlar vermiştir. Ayrıca bilgisayarda "Simpsons.doc" isimli bir dosya açmıştır ve Simpson dizisinden bazı replikleri bu dosyaya yazmıştır. Bu virüs, 80 milyon dolarlık zarar vermiş ve halkta korkuya sebep olmuştur (Polat, 2020).

5.1.4. NATO Siber Saldırısı

NATO, 1999'da gerçekleştirdiği hava saldırısı sonunda Sırp lider Miloseviç'in sonunu getirmiştir. Fakat bu durum birçok eleştirinin de oluşmasına neden olmuştur. Bu eleştiri takiben siber korsanlar NATO' ya siber saldırılar düzenleyerek bilgi sistemlerine sızmışlardır. NATO'nun siber güvenlik açısından zaaflarının ortaya çıkması ile 2002 Prag Zirvesi'nde NATO'nun siber güvenlik politikalarını tekrar gözden geçirilmiştir. Zirve sonunda siber saldırılar olduğu anda ve etkili bir şekilde cevap verilecek bir müdahale merkezi oluşturması kararlaştırılmıştır (Yener, 2014).

5.1.5. World of Hell

World of Hell (ya da kısaca Oh), 2001 yılında birkaç yüksek profilli saldırıdan sorumlu olduğunu iddia eden gri şapkalı bir bilgisayar korsanı grubu olarak bilinmektedirler. Birden çok saldırı gerçekleştirmişlerdir. Saldırıların ardından yüksek profilli hedefleri ve yayınladığı tasasız mesajları nedeniyle dikkat çekmişlerdir. World of Hell özellikle güvenliği düşük web sitelerini bulma ve ardından bir tavsiye mesajıyla siteyi bozma konusunda uzmanlaşmıştır (WayBackMachine, 2001).

5.1.6. Estonya Siber Saldırısı

2007 yılında "Estonya Siber Savaşı" olarak da anılan bu saldırı, küresel ağ internet aracılığıyla gerçekleştirilen en güçlü saldırılardan birisidir. Rus Kızıl Ordusu'nun 2. Dünya Savaşı anısına dikilen "Tallin'in Bronz Heykeli" anıtının yer değiştirilmesi olayı yüzünden ortaya çıktığı ifade edilmiştir. Estonya'da yürütülen bu saldırı o zaman kadar görülmemiş bir saldırı idi ve bu ülkede kurumlarının neredeyse tamamının dijitalleşmiş olması, vatandaşların gündelik birçok işini, internet üzerinden gerçekleştirmesi yüzünden ciddi hasarlar vermiştir (Polat, 2020). Estonya'da yapılan siber saldırılar sonucunda, dünyada uluslararası güvenlik açısından bir dönüm noktası olmuştur. Devlete ait kritik alt yapılara ve önemli bilgilere yönelik yapılan bu saldırı, siber güvenlik politikalarının tartışılmasına neden olmuştur.

5.1.7. Black Energy

İlk olarak 2007 yılında düzenlenen basit bir DDoS saldırısında ortaya çıkmıştır. Akabinde banka dolandırıcılığı ve spam e-posta göndermek için kullanılmıştır. 2014 yılında ise sızdığı bilgisayar sistemlerinde ağda keşfi yapmak, sabit disklerden veri toplamak ve bilgisayarın uzaktan yönetilmesini sağlamak amacıyla arka kapı açmak amaçlı zararlı bir yazılım olarak literatüre geçmiştir (Sertçelik, 2015).

5.1.8. DarkHotel

Kafe veya havalimanlarındaki halka açık Wi-Fi ağlarında görülen zayıf güvenlik politikaları ve güvenlik açıklarından dolayı bazı üst düzey müdür ve çalışanların bilgileri bu gibi ortamlarda çalınmıştır. Bu saldırı ile otelde kalan müşterilere yasal gibi görünen bir güncelleme yükleme gönderilmiştir. Akabinde misafirlerin cihazlarına bu güncelleme ile bir kaç gün içinde DarkHotel casus yazılımı bulaşmıştır. Gizli casus, bir tuş kaydedici ile müşterilerin bütün bilgilerine erişmiş ve siber saldırganların dolandırıcılık yapmalarını sağlamıştır (Drozhzhin, 2014).

5.1.9. Litvanya Siber Saldırısı

Haziran 2008'de üç gün süren bir şekilde Litvanya siber saldırıya uğramıştır. RF temelli olduğu tespit edilen DDoS siber saldırısında Estonya ve Gürcistan'da örnekleri görüldüğü gibi Litvanya'nın önemli altyapı sistemleri DDoS saldırıları ile çökertilmiş ve ülkede en popüler ve en çok kullanılan web sayfalarının ana sayfalarına "orak-çekiç" simgesi koyulmuştur (Ashmore, 2014).

5.1.10. Gürcistan Siber Saldırısı

7 Ağustos 2008 tarihinde Rusya tarafından Gürcistan'a yönelik DDoS siber saldırısı gerçekleşmiştir. Bu saldırılar, önemli altyapıları hedef almıştır. Daha önce Estonya'da görülen siber saldırılara benzemektedir. Saldırılarda kullanılan web siteleri incelendiğinde, bu web sitelerinin ABD'den çalınan kredi kartlarıyla Rusya ve Türkiye'de açıldığı belirlenmiştir. Buna ek olarak saldırıda SPAM e-posta sağanağında oluşturulduğu tespit edilmiştir (Bıçakçı, 2012).

5.1.11. Rocra APT Saldırısı

Kızıl Ekim (Red October) saldırı operasyonunda kullanılan zararlı yazılımın adı Rocra olarak bilinmektedir. Rocra APT saldırısı için gerekli her bir eleman kendine özel

modüller içermektedir: Rocra APT yazılımları en çokta Oracle tabanlı veri tabanlarından bilgi toplayabilmektedir. Amaçları keşif yapma, yayma, devamlılık, veri çekme ve dışarı veri aktarma şeklindedir. Bu zararlı yazılımlar özellikle hem veri dosyalarına hem de veri tabanı kayıtlarına erişim yeteneğine sahiptir. Bunun yanında FTP sunucularına erişim, ağ paylaşımlarının, yerel disk sürücülerinin kontrolü ve bu kaynaklardan dosya kopyalama gibi özellikleri içermektedirler (TerraMedusa, 2013).

5.1.12. Güney Kore Siber Saldırıları

4 Temmuz 2009 tarihinde başlayan siber saldırılarda hedefte ABD Hazine Bakanlığı, İstihbarat Servisi, Federal Ticaret Komisyonu ve Ulaştırma Bakanlığı'nın internet siteleri bulunmaktadır. Bununla birlikte Güney Kore'de bazı resmi kurumlar ve cumhurbaşkanlığı dâhil bazı kurumların sistemlerinin uzun süreler devre dışı bırakılmıştır. Dağıtık Servis Reddi türünde olan bu saldırılarda hedefteki sistem ya da cihazlar devre dışı bırakılmaktadır (BBCTurkish, 2009).

5.1.13. GhostNet

Dünyanın 103 farklı ülkesindeki büyükelçilikleri, dışişleri bakanlıkları gibi makamları hedef alan siber casusluk ağı olarak ortaya çıkmış ve kaynağının Çin olduğu tespit edilmiştir. Çalışma prensibi olarak e-postalar, bağlamsal olarak alakalı bilgiler içeren hedef kuruluşlara gönderilir. Bu e-postalar, açıldığında bir truva atının sisteme erişmesini sağlayan kötü niyetli ekler içermektedir. Bu Truva atı, komutları almak için genellikle Çin'de bulunan bir kontrol sunucusuna geri bağlanmaktadır (Hürriyet, 2011).

5.1.14. Stuxnet

2010’da İran’daki nükleer tesislerde Stuxnet isimli bir solucan yazılımı tarafından bazı kazalar ortaya çıkmıştır. Stuxnet, ABD ve İsrail tarafından İran’ın nükleer faaliyetlerini aksatmak ya da durdurmak için kullandığı bir virüs programı olduğu tespit edilmiştir. Virüsün asıl hedefi ve amacı ise boru hatlarında, nükleer santrallerde, su, elektrik,

kanalizasyon vb. tesislerinin işletilmesinden sorumlu olan SCADA adlı mekanizmadır (Holat, 2021).

5.1.15. GoDaddy Saldırısı

İnternet ‘domain' hizmeti veren GoDaddy'ye yönelik siber saldırıda neredeyse 1.2 milyon müşterinin telefon numarası ve e-posta adresinin bilgileri ele geçirilmiştir. Saldırının kaynağı olarak şirketin WordPress tabanlı yönetim sistemi gösterilmiştir. Saldırganlar saldırı sırasında, şirketin WordPress tabanlı yönetim panellerindeki yönetici şifrelerini de ele geçirmiştir.

5.1.16. CryptoLocker

5 Eylül 2013 tarihinde Microsoft Windows işletim sistemlerini hedef alan CryptoLocker, fidyeci truva atı olarak bilinmektedir. CryptoLocker, virüslü e-posta ile gönderilen eklerden bilgisayar sistemlerine sızmış, bilgisayar ağları ve sistemlerinde yer alan depolama aygıtlarındaki bazı dosyaları şifrelemektedir. Akabinde kullanıcıya şifreli dosyaların çözülmesi için yüksek miktarda ödeme yapılmasını teklif eden bir fidye mesajı gönderilmektedir. Fidyeciler belirlenen süre içerisinde istedikleri bitcoin ödemesi yapılmadığı takdirde şifreli dosyaların geri getirilemeyeceği tehdidinde bulunulmuştur.

5.1.17. Kill Disk

Çoğunlukla Ukrayna ve Polonya’daki birçok özel kurum, devlet kuruluşu ve sivil organizasyonların bilgisayarlarında tespit edilmiştir. Örnek olarak Kill Disk truva atı ve Black Energy birlikte 23 Aralık 2015 tarihinde Ukrayna’da enerji dağıtım şirketine düzenlenen siber saldırıda isminden söz ettirmiştir (Çeliktaş, 2016).

5.1.18. Ukrayna Siber Saldırısı

23 Aralık 2015’de Ukrayna’nın Ivano-Frankivsk bölgesinde elektrik dağıtım şirketine siber saldırı düzenlenmiştir. 700 bin kişinin etkilendiği saldırıda saatlerce elektrik

kesintisi yaşanmıştır. Saldırıda BlackEnergy truva atı ile birlikte KillDisk truva atıda kullanılmış ve saldırının etkisi arttırılmıştır (Hürriyet, 2016).

5.1.19. Mirai

21 Ekim 2016'da ABD'de en önemli sitelere giriş engellenmiştir. Sosyal ağ sitelerine, Amazon, Spotify ve bazı çevrimiçi oyunlara erişilememiştir. Sebebi olarak DNS sunucularına yönelik bir DDoS saldırısı gösterilmiştir. DDoS saldırısında bu sefer botnetler, klasik bilgisayarlar haricinde Nesnelerin İnterneti teknolojisi ile çalışan cihazlar üzerinden de saldırı düzenlenmiştir. Böylelikle, 21 Ekim 2016'da, botnetlerden kurulu dev bir zombi taburu DDos saldırısına geçmiştir. Milyonlarca dijital video kaydedici, yönlendirici, IP kamerası ve diğer akıllı cihazların DNS servis sağlayıcısı Dyn istek bombardımanına tutulmuştur. Dyn ise bu saldırı sonucunda kullanılmaz hale gelmiştir. Ayrıca bundan PayPal, Twitter, Netflix, Spotify ve PlayStation çevrimiçi hizmetleri gibi uygulamalar etkilenmiştir. Akıllı cihazların katılımı ile düzenlenen saldırı sebebiyle nesnelerin interneti teknolojisi ile çalışan cihazların güvenliği ön plana alınmıştır (Kochetkova, 2016).

5.1.20. Atlanta Siber Saldırısı

2016 yılının Ekim ayında NSA tarafından kullanılan hack araçlarını çalındığı iddia edilmiştir. Akabinde NSA bağlantılı grup olan Equation tarafından sızmanın gerçekleştiği sunucuların özelliklerini barındıran bir liste yayınlamıştır. Saldırıların belgelerini yayınlayan grup ele geçirilen verileri açıklamamak karşılığında NSA'dan bir milyon bitcoin istemiştir.

5.1.21. NotPetya / ExPetr

12 Mayıs 2017'de Türkiye'de dâhil tüm Avrupa bölgesini hedef alan büyük çaplı bir fidye için siber saldırı gerçekleşmiştir. Günümüze kadar en maliyetli yapılan saldırı olarak görülmektedir. Yetkisi erişim programları kullanan bu solucan ağda gezinerek öne çıkan her şeyi geri dönülemez şekilde şifrelemiştir. Siber suçlular bilgisayarlardaki verileri çözmek

için üç yüz dolar karşılığı bitcoin istemiştir. Bu saldırının zararının on milyon dolar olduğu tahmin edilmektedir (Hürriyet, 2017).



Şekil 5.1. NotPetya Saldırısı (Heavy, 2017)

5.1.22. WannaCry

12 Mayıs 2017 başlayıp 4 gün içerisinde Wannacry saldırısı 150 ülkede 200.000'den fazla sisteme zarar vermiştir. Son yapılan saldırılar arasındaki en geniş kapsamlı yapılan saldırı olmuştur. Bu kötü amaçlı yazılım iki kısımdan oluşmaktadır. Trojan yazılımı eki ve yamalanmamış Windows sistemlerindeki SBM güvenlik açıklarını araştırarak sızma işlemi gerçekleştirirken, diğer kısımda ise sızılan bilgisayar sistemindeki bütün dosyalar şifrelenerek WNCRY uzantısı ile tekrar kaydedilmiştir. Böylece yazılım her dizinde bir fidye oluşturarak ve arka planda resminde kurbandan istenen ödeme miktarı bir text mesajı ile belirtilmektedir (Sağıroğlu ve Alkan, 2018).



Şekil 5.2. WannaCry Saldırısı (BBC, 2017)

5.1.23. US Universities

Mart 2018'de ABD Adalet Bakanlığı, 9 İranlı siber saldırganı 300'den fazla üniversitede düzenlenen siber saldırıdan sorumlu tutulmuştur. 21 ülke,176 üniversite,47 özel şirket, Birleşmiş Milletler, ABD Federal Enerji Düzenleme Komisyonu ile Hawaii ve İndiana gibi diğer hedef alınan yerlere sızmakla suçlanmaktadırlar. DOJ, korsanların üç milyar dolar değerinde 31 terabaytlık veri çaldığını rapor etmiştir. Saldırılar; üniversitedeki çalışanlar tarafından, kötü niyetli bağlantıları tıklamaları ve ağa giriş kimlik bilgilerini girdirmeyi hedeflenen özenli e-postalar kullanılmıştır (WIRED, 2018).

5.1.24. Github

Dünyadan birçok geliştiricinin kodlarını barındıran GitHub, internet tarihinin en büyük DDoS saldırısına uğramıştır. Bu saldırıda saniyede 1.35 terabitlik veri akışı sağlanmış ve neredeyse 10 dakika boyunca GitHub'ın erişilebilirliği engellenmiştir. Bu saldırıdan 4 gün sonra rekor kırılarak 1.7 terabitlik istek ile saldırı tekrarlanmıştır. Fakat yetkililer bu saldırıyı geri püskürterek sitenin tekrar hizmete girmesi sağlanmıştır. Bu saldırıda botnetler yerine

github ip adresini kullanarak TCP/IP paketleri oluşturup, birden fazla memcached sunucusuna web sorgusu gönderilmiştir (Siber Bülten, 2018).

5.1.25. Rampant Veri Sızıntısı

2018 yılında Exactis isimli firma yaklaşık 340 milyon veriyi herkese açık bir sunucu üzerinde güvenlik ve gizlilik önlemi almamış bir şekilde bırakmıştır. Sızdırılan verilerin içeriğinde sosyal güvenlik numaraları veya kredi kart bilgileri vardı. Bu verilerin çoğunluğu Amerikalı gençlere ait olup, 2 terabytelık bilgi kapasitesine sahiptir (Sağıroğlu ve Alkan, 2018).

5.1.26. Almanya Siber Saldırısı

11 Eylül 2020 tarihinde Düsseldorf'da yerel bir hastanede bilgisayar korsanlarının verileri şifrelediği ve akabinde verilerin şifresini çözmek için ödeme talep ettiği bir fidye yazılımı saldırısı gerçekleştirdikleri için süreçlerin durmasından dolayı hastanenin ambulansı geri çevirmeye zorladığı tespit edilmiştir. Saldırı, hastanenin doktorları, yatakları ve tedaviyi koordine etmek için güvendiği dijital altyapıyı tehlikeye atarak yüzlerce operasyonu ve diğer prosedürleri iptal etmeye de zorlamıştır (CyberArts,2021).

5.1.27. İsrail Siber Saldırısı (Black Shadow)

İsrail'in Başbakanlık resmi internet sitesinin yanı sıra İçişleri, Sağlık, Adalet ve Sosyal İşler Bakanlıklarının sitelerine yönelik "Black Shadow" adlı grup tarafından bir siber saldırı düzenlenmiştir. Bu grup eylemlerine ilk olarak Aralık 2020'de İsrail sigorta şirketi Shirbit'e düzenlediği saldırıyla başlamıştır. Akabinde İsrail'e ait birçok internet sitesine saldırı düzenlenmiştir. Fakat 6 Kasım 2021'de İsrail'in Cyberverse adlı hosting şirketine düzenlenen siber saldırı grubun en büyük saldırısı olarak internet tarihine geçmiştir. Siber saldırganlar bu saldırı ile İsrail'de eşcinsellerin kullandığı "Atraf" adlı sosyal ağ uygulama platformunu kullanan kişilerin kimlik bilgilerini ele geçirmişlerdir. Bunun karşılığında fidye

talep etmişler ve bu talepleri karşılanmaz ise bu bilgileri internette yayınlama tehdidinde bulunmuşlardır.

5.1.28. İrlanda Siber Saldırısı

Fidye yazılımı saldırıları sonucunda 2021 yılında İrlanda sağlık sistemi sekteye uğramıştır. Sistemler siber saldırıdan korunamadığı için ciddi oranda para kaybı yaşanmıştır. Saldırıda fidye yazılımı aktifleştirmeden önce iki ay boyunca tespit edilememiştir. Siber saldırganlar öncelikle oltalama saldırısıyla sağlık sisteminin ağında arka kapı bağlantısı kurduğu ve uzaktan erişim araçlarıyla sistemde hareket etmişlerdir (Savunmatr, 2022).

5.1.29. PseudoManuscrypt

PseudoManuscrypt, ilk olarak Aralık 2021'de Rus siber güvenlik firması Kaspersky tarafından dünya çapında 195 ülkede 35.000'den fazla bilgisayara bulaşan bir "kitlesel casus yazılım saldırısı kampanyasının" ayrıntılarını açıkladığı zaman belgelenmiştir. İlk olarak Haziran 2021'de ortaya çıkardığı PseudoManuscrypt saldırılarının hedefleri arasında Rusya, Hindistan ve Brezilya'daki askeri-sanayi kompleksi ve araştırma laboratuvarlarındaki işletmeler de dâhil olmak üzere önemli sayıda sanayi ve devlet kuruluşu yer almaktadır (Lakshmanan, 2022).

5.1.30. Norveç Siber Saldırısı

Ocak 2022 yılında Norveç'e yönelik bir siber saldırı gerçekleşmiştir. Bu siber saldırı bir gün içerisinde Norveç'teki kamu ve özel web sitelerini geçici olarak devre dışı bırakmıştır. Norveç Ulusal Güvenlik Otoritesi, DDoS saldırısının güvenli bir ulusal veri ağını hedef alarak çevrimiçi hizmetlerin birkaç saat süreyle geçici olarak askıya alınmıştır (Cnbc, 2022).

Çizge 5.1. Dünya Üzerinde Yapılmış Siber Saldırı Örnek Listesi

Saldırı Numarası	Saldırı Adı	Saldırı Yılı	Saldırı Yapılan Ülke	Saldırı Hedefi	Saldırı Türü
1	Sibirya Siber Saldırısı	1982	Rusya	Doğalgaz Boru Hattı	Mantık Bombası/ Truva Atı
2	Moonlight Moze	1998	ABD	Nasa, Pentagon ve Amerikan Devlet Kurumları	Casus Yazılımlar/ Backdoor
3	Melisa	1999	UseNet (Worldwide Distributed Discussion System)	E-posta Sunucuları/ Donanımlar	Virüs/Solucan
4	Nato Siber Saldırısı	1999	NATO	NATO Güvenlik ve Savaş Sistemleri	DDoS
5	World of Hell	2001	Dünya Geneli	Büyük Şirketlerin Web Siteleri	DDoS
6	Estonya Siber Saldırısı	2007	Estonya	Devlete Ait Kritik Altyapılar ve Kurumlar	DDoS
7	Black Energy	2007	Gürcistan	Gürcistan'daki Bir Norveç bankası ve Hükümet Web Siteleri	Truva Atı/Botnet/DDoS
8	DarkHotel	2007	Güney Kore	Üst Düzey Şirket Yöneticilerini	Casus Yazılımı
9	Litvanya Siber Saldırısı	2008	Litvanya	Devletin Kritik Altyapıları	DDoS
10	Gürcistan Siber Saldırısı	2008	Gürcistan	Devlete Ait Kritik Altyapılar ve Kurumlar	DDoS / Spam E-Posta

11	Rocra APT Saldırısı	2008-2013	Doğu Avrupa'daki Belirli Örgütler, Eski SSCB Ülkeleri ve Orta Asya'daki Ülkeler	E-posta Veri Tabanları	Casus Yazılım
12	Güney Kore Siber Saldırıları	2009	Güney Kore ve ABD	Hükümet, Haber Medyası ve Finans Siteleri	DDoS/Botnet
13	GhostNet	2009	103 Ülke	Büyükelçilikler, Dışişleri Bakanlıklarına ve Diğer Devlet Dairelerine Ait Bilgisayar Sistemleri	Truva Atı
14	Stuxnet	2010	İran	Nükleer Tesis	Solucan
15	GoDaddy Saldırısı	2012	Dünya Geneli	Web Hosting Şirketine	DDoS
16	CryptoLocker	2013	ABD ve İngiltere	MS Windows İşletim Sistemli Bilgisayarlar	Fidye Yazılımı /Truva Atı
17	Kill Disk	2015	Ukrayna/Polonya	Özel ve Devlet Kurumları ve Sivil Organizasyon	Truva Atı
18	Ukrayna Siber Saldırısı	2015	Ukrayna	Enerji Dağıtım Şirketleri ve Haber Ajansları	DDoS/Truva Atı
19	Mirai	2016	Çin, Güney Kore, Amerika	Görüntü Sistemleri (25 Bin Kameranın Görüntüsü)	DDoS
20	Atlanta Siber Saldırısı	2016	Atlanta/Georgia	Kamu ve Mahkeme Hizmetleri	Fidye Yazılımı
21	NotPetya/ExPetr	2017	Avrupa	Avrupa Temelli Ağa Bağlı Bilgisayarlar	Fidye Yazılımı/Solucan
22	WannaCry	2017	150 ülke	MS Windows İşletim Sistemli Bilgisayarlar	Fidye Yazılımı/ Truva Atı

23	US Universities	2018	21 Ülke	Özel şirket, Birleşmiş Milletler, ABD Federal Enerji Düzenleme Komisyonu ile Hawaii ve İndiana	Truva Atı/Solucan
24	Github	2018	Dünya geneli	Küresel Çapta Hizmet Geliştiriciler ve Yazılımcılar Platformu	DDoS
25	Rampant Veri Sızıntısı	2018	ABD	Exactis Adlı Şirket	Casus Yazılım
26	Almanya Siber Saldırısı	2020	Almanya /Düsseldorf	Sağlık Sistemleri	Fidye Yazılımı
27	İsrail Siber Saldırısı (Black Shadow)	2021	İsrail	İsrail'in Cyberverse Adlı Hosting Şirketine	Fidye Yazılımı
28	İrlanda Siber Saldırısı	2021	İrlanda	Sağlık Bakanlığı	Fidye Yazılımı
29	PseudoManuscrypt	2021	Rusya, Hindistan, Brezilya, Vietnam ve Endonezya	Endüstriyel Kontrol Sistemleri	Casus Yazılım/Keylogger
30	Norveç Siber Saldırısı	2022	Norveç	Kamu ve Özel Web Siteleri	DDoS

Çizge 5.1'de yer alan dünya genelinde yapılan siber saldırılar incelendiğinde çoğunlukla ülkelerin enerji ve sağlık sistemlerinin hedef olduğu görülmüştür. Saldırı teknikleri açısından ise DDoS, Fidye yazılımları ve Trojanlar'ın daha çok kullandığı tespit edilmiştir. Aynı zamanda birçok saldırıda bazı saldırı teknikleri beraber kullanılmıştır. Bulgular göstermektedir ki; siber savaşların arttığı siber dünyada özellikle dijital paralar ile

finansman sağlamak ve son dönemde dünyada kıymetli hale gelen doğalgaz ve nükleer tesisler gibi enerji üretimini duraksatmak ya da engellemek nihai amaç haline gelmiştir.

Bu incelenen siber saldırıların 18 tanesi kritik altyapılara karşı gerçekleştirilmiştir. 12 tanesi diğer kurumlara karşı yapılmıştır.

5.2.Türkiye'den Siber Saldırı Örnekleri

Tez çalışmasında bir önceki kısımda dünya üzerinde öne çıkmış ve hasarları geniş olan siber saldırılar ele alınmıştır. Bu bölümde ise dünyada gerçekleşip Türkiye'ye de etkisi olan ya da direkt olarak Türkiye'deki özel ya da devlet kurumlarını hedef alan ve kamuoyunda ses getiren siber saldırı örnekleri ele alınacaktır. Burada tarihsel olarak sıralanmış şekilde 15 adet siber saldırı örneğine yer verilmiştir. Siber saldırıların hangi amaçla yapıldığı, nereye yapıldığı ve hangi yöntem ile yapıldığı verilmiştir.

5.2.1. Bakü-Ceyhan-Tiflis Boru Hattı Saldırısı

5 Ağustos 2008 tarihinde Bakü-Tiflis-Ceyhan boru hattı üzerinde Erzincan'ın Refahiye ilçesi yakınlarında bir patlama meydana gelmiştir. İlk zamanlarda bir terör saldırısı olarak lanse edilen patlamanın sebebinin sofistike bir siber saldırısı olduğunu öne sürülmüştür Patlamada kullanılan silahın 'klavye' ile yapılmış mantık bombası şeklinde olduğu dile getirilmiştir. Virüslerinde saldırıda kullanıldığı ve güvenlik kameralarından sisteme girilerek, alarm sistemlerinin etkisiz hale getirildiği aktarılmıştır (Cumhuriyet, 2014; Şenol, 2016).

5.2.2. Conficker

30 Ocak 2009 tarihinde birçok ülkede eş zamanlı bilgisayarlara bulaşan ve ciddi hasarlar veren Conficker virüsü aynı zamanda Türkiye'de de Atatürk Havalimanı'nın dış hatlar terminalinde çalışan bilgisayarlara bulaşmıştır. Saldırı yüzünden yolcu bagaj işlemleri ertelenmiş, yolcular arasında kargaşa ve uzun kuyruklar oluşmuştur (Karabacak, 2011).



Şekil 5.3. Confiker Saldırısı (Wikipedia, 2022)

5.2.3. Türkiye İletişim Başkanlığına (TİB) Yönelik Siber Saldırı

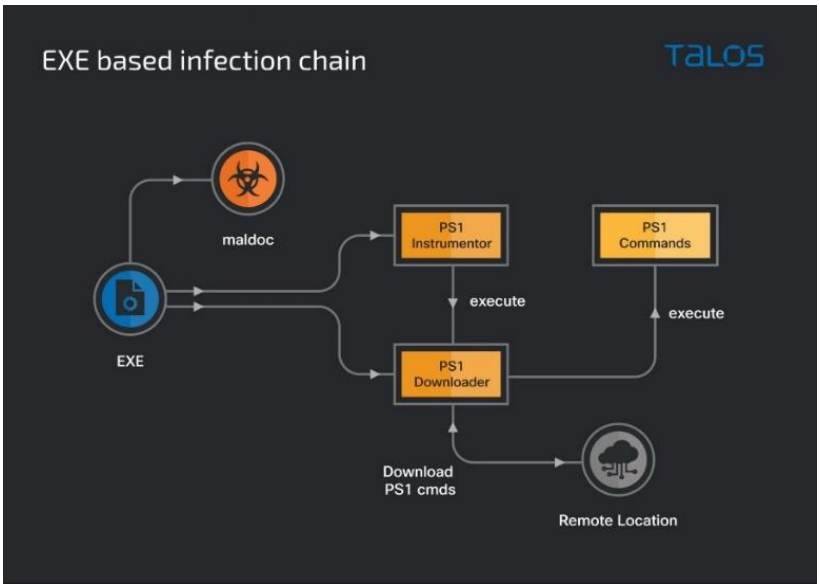
Haziran 2011'de BTK Telekomünikasyon İletişim Başkanlığının internet sitesine siber saldırı düzenlenmiştir. İnternete Filtre Uygulamasının karşısında temel hak ve özgürlüklerin ihlal edileceğini savunan "Anonymous" adlı Uluslararası Bilgisayar Korsanları Topluluğu tarafından yürütülen saldırıda etkilenen ve çalışması duran web sitesi ancak gece yarısından sonra aktif hale gelebilmiştir (Şenol, 2012).

5.2.4. Sağlık Bakanlığına Yönelik Siber Saldırı

Mayıs 2016 tarihinde Sağlık Bakanlığı Hastanelerine siber saldırı düzenlenmiştir. Diyarbakır, Siirt, Tekirdağ ve Kocaeli illerinde faaliyet gösteren bazı hastanelere yönelik siber saldırılar sadece Diyarbakır ilindeki hastanede kısmen etkili olmuştur. Siber saldırıda ilgili hastanelerin bilgi sistemlerindeki kısmi aksama sebep olmuştur (Sağlık Bakanlığı, 2016).

5.2.5. Muddy Water (APT) Siber İstihbarat Saldırısı

2018 yılında Muddy Water Advanced Persistent Threat (APT - Gelişmiş Sürekli Tehdit) grubunun Türkiye'ye yönelik saldırıları tespit edilmiştir. Zararlı e-postalar ile yürütülen oltalama şeklindeki siber saldırıda, bu e-postaları alan kullanıcıların Macro desteğini açtırmaya yönelik yönlendirme yapılmaktadır. Makroları aktif hale getiren kullanıcıların bilgileri ele geçirilmektedir (Havelsan, 2018).



Şekil 5.4. Muddy Water (APT) Saldırısı (Malhotra, 2022)

5.2.6. Türk Telekom'a Yönelik Siber Saldırı

20 Ocak 2020 tarihinde Türkiye'de faaliyet gösteren en büyük Telekomünikasyon şirketi Türk Telekom'a DDoS saldırısı düzenlenmiştir. Bu siber saldırılar yüzünden internette kesilmeler yaşanmıştır. Siber saldırılar Türk Telekom'un DNS'lerine yönelik yapılmaktadır. Bu saldırıda 100 GB miktarında DDoS tekniği kullanılmıştır (Haberturk, 2020).



Şekil 5.5. Türk Telekom'a Siber Saldırı (Habertürk, 2020)

5.2.7. Yemeksepetine Yönelik Siber Saldırı

18 Mart 2021 tarihinde Yemeksepeti firmasına, veri tabanı sorumlusu tarafından kimliği tespit edilemeyen şahıs ya da şahıslarca bir siber saldırı düzenlenmiştir. Bu siber saldırıda Yemek Sepetine ait bir web uygulama sunucusuna erişilmiştir. 21 milyon 504 bin 83 kişinin etkilendiği bu siber saldırı sonucunda uygulama sitesinin kullanıcı veri tabanı ele geçirilmiştir. Rusya menşeili saldırıda bilgisayar korsanları bilgilerin paylaşılmaması adına fidye olarak 5 bitcoin fidye istemişlerdir (Usta, 2021).

5.2.8. Konya Büyükşehir Belediyesine Yönelik Siber Saldırı

2021 yılında Yemeksepeti'ne düzenlenen siber saldırıya benzer şekilde Konya Büyükşehir Belediyesi siber saldırıya uğramıştır. 29 Mart 2021 tarihinde yaşanan siber saldırıda siber korsanlar aralarında belediye çalışanları ve belediyeye mail atan vatandaşların da bulunduğu 1 milyona yakın kişinin T.C kimlik numaraları ve diğer kişisel bilgilerini ele geçirmişlerdir. Bu veriler bir hacker forum sitesinde saldırgan ya da saldırganlar tarafından satılığa çıkarılmıştır (Sputnik, 2021).



Şekil 5.6. Saldırıda Çalınan Veriler (SonDakika, 2021)

5.2.9. Medlife Sağlık Kurumuna Yönelik Siber Saldırı

15 Mart 2022 tarihinde Türkiye'de üç hastanesi ve üç kliniği bulunan Medilife Sağlık Grubu adıyla faaliyet gösteren Yonca Sağlık Hizmetleri Ltd. Şti.'nde gerçekleşen siber saldırıda, yaklaşık 500 bin hastanın kişiye ait 2,5 milyon veri ele geçirilmiştir. Saldırı direkt olarak veri sorumlusu sistemlerini hedef almıştır. Saldırı veri tabanı sorumlusuna veya bilgi işlem müdürüne gönderilen bir e-posta ile ortaya çıkmıştır (Medilife, 2022).

5.2.10. Pegasus Siber Saldırısı

Mart 2022 tarihinde Türk uçuş operatörü Pegasus Havayolları veri ihlali yaşamıştır. Türk uçuş operatörü Pegasus Airlines, bir AWS bulut depolama paketinin korumasız bırakıldığı bildirmiştir. Yüksek miktarda müşteriye ait Elektronik Uçuş Çantası (EFB) bilgilerinin açık bir şekilde saklandığı ve hassas bilgilere erişime izin verildiği bildirmiştir. Türkiye'nin veri koruma kurumu saldırıdan sonra şirketten bir veri ihlali bildirimi almış ve bir sızıntı olduğunu doğrulamıştır (Haworth, 2022).

5.2.11. ALtahrea Saldırısı

Nisan 2022 tarihinde Shafaq News/Dijital Medya Merkezi (DMC), ALtahrea Ekibi tarafından Irak topraklarına DDoS saldırısı yapılmıştır. Irak'tan yapılan bu siber saldırının Cumhurbaşkanlığı web siteleri de dâhil olmak üzere Anadolu Haber Ajansı ve Türk ordusuna bağlı bir uçak şirketin web siteleri hedef alınmıştır (Shafaq News, 2022).

5.2.12. Baydöner Restorana Yönelik Siber Saldırı

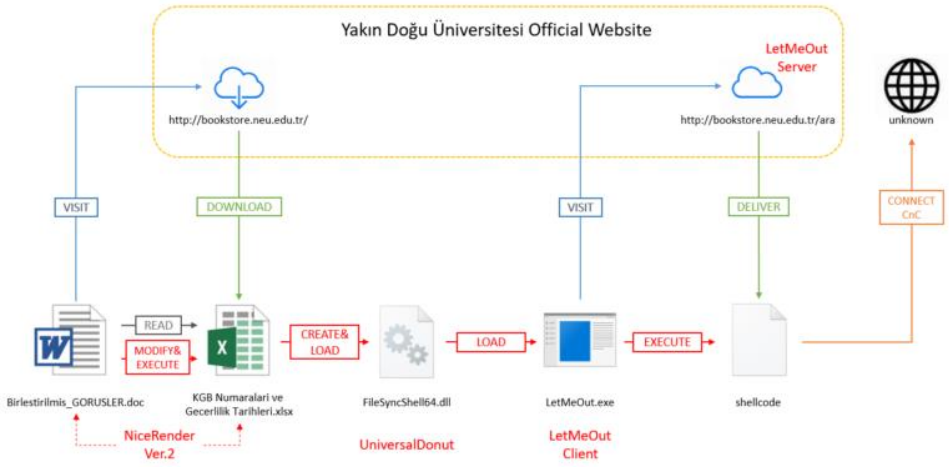
2022 yılı Mayıs ayı içerisinde İzmir merkezli restoran zinciri Baydöner'e siber saldırı düzenlenmiştir. Saldırı, veri tabanı yöneticisi ve Bilgi İşlem yöneticisine ait bilgisayarların kötücül bir yazılım ile saldırıya uğraması sonucunda web servis şifrelerinin ele geçirilmesi ile sonuçlanmıştır. Siber saldırıda 505 binden fazla kullanıcının kişisel bilgilerinin ele geçirilmiştir (Karakış, 2022).

5.2.13. Tübitak'a Yönelik Siber Saldırı

Ağustos 2022 tarihinde Çinli siber güvenlik şirketi NSFocus'un raporuna göre TÜBİTAK'ın defalarca siber saldırıya uğradığı duyurmuştur. Bu saldırı ile e-postalar üzerinden gönderilen çeşitli teknik dokümanlar ele geçirilmiştir. Ayrıca siber saldırganlar, TÜBİTAK personelinin cihazlarına trojanlar ile sızarak e-posta görüşmelerini, kimlik bilgilerini ve tarayıcı ön belleklerini ele geçirmiştir (Akbaş, 2022).

5.2.14. MurenShark

Ağustos 2022 tarihinde MurenShark isimli bir hacker grubu tarafından milli denizaltı yönetim sistemi MÜREN'e siber casusluk operasyonları gerçekleştirilmiştir. MurenShark tarafından MÜREN'in kritik tasarım dokümanları ve sürüm tanımlama sistemine ilişkin önemli belgeleri ele geçirilmiştir. Saldırı aracı olarak UniversalDonut ve LetMeOut casus yazılımları kullanılmıştır (Akbaş, 2022).



Şekil 5.7. MurenShark Saldırısı (Ji, 2022)

5.2.15. THY Saldırısı

Temmuz 2022 tarihinde tanınmış bir Dijital Medya Merkezi, bir siber saldırının Türk Hava Yolları(THY) web sitesini bozduğunu doğrulamıştır. Irak Haber Ajansı'na (INA) gelen kısa bir açıklamada DDoS saldırısı ile THY'nin internet sitesinin erişime engellendiği ve saldırıyı bir Irak ekibinin üstlendiği ifade edilmiştir (Iraqi News Agency, 2022).

Çizge 5.2. Türkiye'ye Yönelik Yapılmış Siber Saldırı Örnekleri Listesi

Saldırı Numarası	Saldırı Adı	Saldırı Yılı	Saldırı Yapılan Ülke	Saldırı Hedefi	Saldırı Türü
1	Bakü-Tiflis-Ceyhan Boru Hattı Saldırısı	2008	Azerbaycan , Türkiye, Gürcistan	Petrol ve Doğalgaz Tesisleri	Mantık Bombası /Virüs
2	Conficker	2009	Türkiye ve Dünya Geneli	İstanbul Havalimanı Dış Hatlar	Virüs
3	TİB'e Yönelik Siber Saldırı	2011	Türkiye	TİB'e Bağlı Web Siteleri	DDoS
4	Sağlık Bakanlığı Hastanelerine Yönelik Siber Saldırı	2016	Türkiye	33 Devlet Hastanesi	Veri Hırsızlığı (Casus Yazılım)
5	Muddy Water (APT)	2018	Irak,Suudi Arabistan, Afganistan, Pakistan ve Türkiye	Kamu ve Askeri Kurumların, Telekom Şirketlerinin ve Eğitim Kurumları	Oltalama Tekniği
6	Türk Telekoma Yönelik Siber Saldırı	2020	Türkiye	DNS Servisleri	DDoS
7	Yemek Sepetine Yönelik Siber Saldırı	2021	Türkiye	Müşteri Veri Tabanı	Fidye Yazılımı/Veri Hırsızlığı/ Backdoor
8	Konya Büyükşehir Belediyesine Yönelik Siber Saldırı	2021	Türkiye	Kurum Veri Tabanları	Fidye Yazılımı/Veri Hırsızlığı/ Backdoor
9	Medlife Sağlık Kurumuna Yönelik Siber Saldırı	2022	Türkiye	Hasta Bilgileri İçeren Veri Tabanı	Veri Hırsızlığı/Back Door
10	Pegasus Siber Saldırısı	2022	Türkiye	Müşteri Bilgileri	Backdoor

11	ALtahrea Saldırısı	2022	Türkiye	Türkiye Cumhurbaşkanlığı, Anadolu Haber Ajansı ve Türk Ordusuna Bağlı Bir Uçak Şirketi	DDoS
12	Baydöner Restoran Yönelik Siber Saldırı	2022	Türkiye	Web Servis Şifreleri	Malware Yazılım
13	TÜBİTAK Saldırısı	2022	Türkiye	E-posta Hesapları	Trojan
14	MurenShark	2022	Türkiye	Milli Denizaltı Yönetim Sistemi-Müren	Casus Yazılım-Trojan
15	THY Saldırısı	2022	Türkiye	Müşteri Bilgileri	DDoS

Çizge 5.2'de yer alan Türkiye'deki kurumlara yapılan siber saldırılar incelendiğinde dünya genelinde olduğu gibi çoğunlukla saldırı tekniklerinin DDoS, Fidye yazılımları ve Trojanlar olduğu görülmektedir. Hedeflerin genellikle özel şirketlerin müşteri bilgilerini elde etmek ve ülke genelindeki iletişim kanalları olduğu görülmüştür. Türkiye'ye yönelik yapılan siber saldırıların devlet organlarından ziyade özel sektör üstünde yoğunlaştığı anlaşılmaktadır. Bunun sebebi olarak Türkiye'nin siber güvenlik açısından son zamanlarda uzun yol kat ettiği açısından değerlendirilebilir (Altun, 2022). Ayrıca Dünya ve Türkiye genelinde yapılan saldırılar ülkeler arasındaki diplomatik ve ekonomik anlaşmazlıkların bir sonucu olarak siber savaşların arttığını göstermektedir.

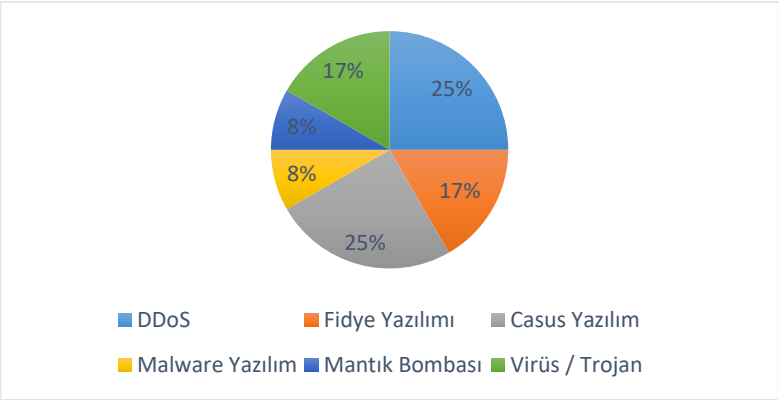
Bu incelenen siber saldırıların 11 tanesi kritik altyapılara karşı gerçekleştirilmiştir. 4 tanesi diğer kurumlara karşı yapılmıştır.

BÖLÜM 6

SONUÇ VE TARTIŞMA

İnternetin keşfiyle birlikte günlük hayattaki verilerin sanal ortama hızla aktarılmasıyla, siber alanların genişleyerek bu ortamdaki güvenliğin ne kadar önemli olduğu ortaya çıkmaktadır. Dünya üzerinde siber alanda, yeni yıkıcı uygulamalar geliştirilmeye devam etmektedir. Siber güvenlik, bu tür saldırılara karşı savunma için alınabilecek tüm güvenlik önlemlerini kapsamakta olup, son yıllarda siber saldırıların gelişmişliği ve şiddetinin gözle görülür biçimde artmıştır. Son yıllarda gerçekleşen siber saldırıların sonuçları, gerçekleşmesi muhtemel saldırıların büyüklüğü ve yıkıcılığı konusunda bize fikir vermektedir. Örneğin bir virüs tarafından bireylerin hatta şirketlerin finans kayıtlarının yok edilebilmesi, bir virüsün tüm borsanın durmasına sebep olacak şekilde çalışamayacak hale getirmesi, hatalı bir mesaj veya dışarıdan bir müdahalenin nükleer tesisisin çalışmasını durdurması hatta uçakların, barajların kapaklarını açabilmesi, havaalanı trafik sisteminin karıştırılması sonucu uçak kazalarının yaşanması gibi hem fiziksel hem de ekonomik zararlara sebebiyet verebileceği hatta daha ileri boyuta ulaşarak can kayıplarına neden olabileceğini bize göstermektedir.

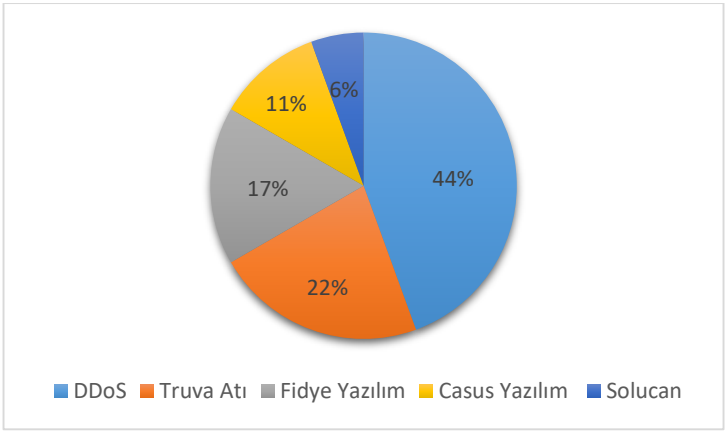
Siber alanlarda yapılan bu saldırıların önlenebilmesi için saldırı tipine göre doğru korunma yöntemlerinin seçilebilmesi önem arz etmektedir. Çizge 5.1.'de verilen Dünya üzerinde gerçekleşen siber saldırı örneklerinde kullanılan siber saldırı yöntemlerinin kullanılma oranı aşağıdaki grafikte gösterilmiştir.



Şekil 6.1. Dünya'da Gerçekleşen Siber Saldırı Türü Oranları

Şekilde görüldüğü gibi en çok kullanılan saldırı yöntemleri DDoS ve Casus Yazılım olduğu tespit edilmiştir. Bu iki siber saldırı yönteminin ortak amacı sistemin çalışmasının engellenmesi ya da sisteminin yavaşlatarak, hizmetin engellenmesi hedeflenmektedir. Bu iki saldırı yöntemine karşı kullanılacak korunma yöntemi en iyi Firewall ve IDS /IPS'dir.

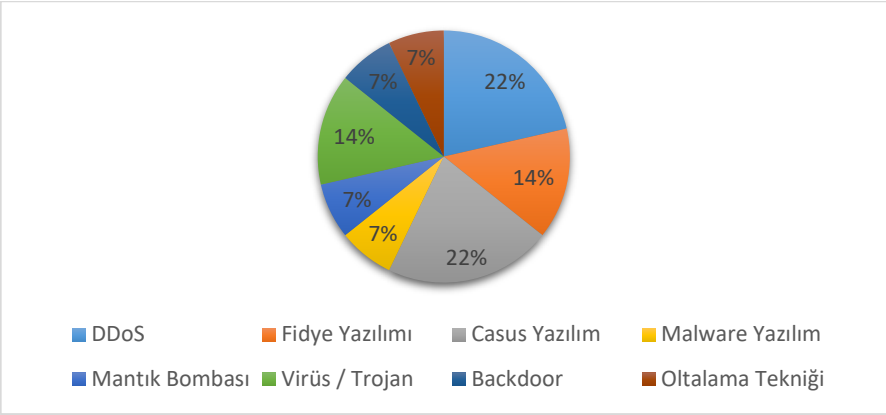
Çizge 5.1'de verilen Dünya'da kritik altyapılara yönelik gerçekleşen siber saldırı örneklerinde kullanılan siber saldırı yöntemlerinin kullanılma oranı grafikte gösterilmiştir.



Şekil 6.2. Dünya'da Kritik Altyapılara Yönelik Gerçekleşen Siber Saldırı Türü Oranı

Şekilde görüldüğü gibi en çok kullanılan saldırı yöntemleri DDoS ve Truva Atı olduğu tespit edilmiştir. DDoS yönteminde sistemin çalışmasının engellenmesi ya da sisteminin yavaşlatarak, hizmetin engellenmesi hedeflenirken, kötü amaçlı yazılım türü olan Truva Atı kişilerin izni olmadan bilgisayar sistemlerine sızmaktır. Bu iki saldırı yöntemine karşı kullanılacak korunma yöntemi en iyi Firewall, IDS /IP ve Antivirüs yazılımıdır.

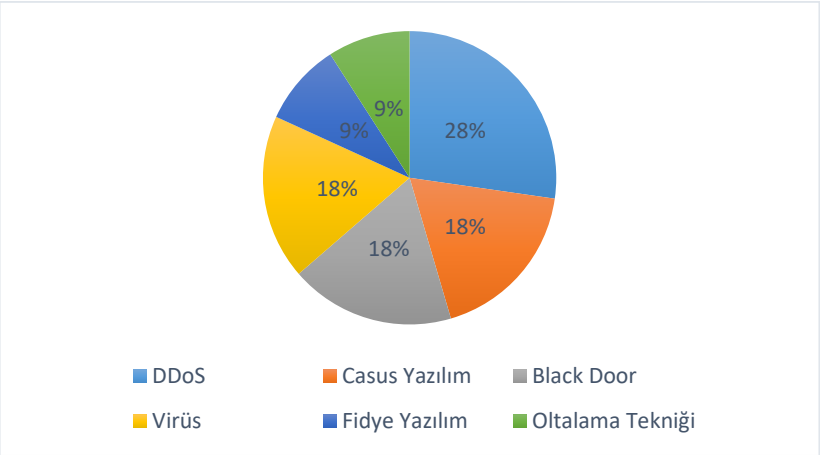
Çizge 5.2.'de listesi verilmiş olan Türkiye üzerinde gerçekleşen siber saldırı örneklerinde kullanılan siber saldırı yöntemlerinin kullanılma oranı ise aşağıdaki grafikte gösterilmiştir.



Şekil 6.3. Türkiye'de Gerçekleşen Siber Saldırı Türü Oranları

Şekilde görüldüğü gibi en çok kullanılan saldırı yöntemleri DDoS ve Casus Yazılımı olduğu tespit edilmiştir. DDoS yönteminde sistemin çalışmasının engellenmesi ya da sisteminin yavaşlatarak, hizmetin engellenmesi hedeflenirken, Casus Yazılım yönteminde bilgisayarınıza izniniz olmadan yüklenen bir yazılımla birçok veriniz elde edilmektedir. Bu iki saldırı yöntemine karşı kullanılacak en iyi korunma yöntemi Firewall, IDS /IPS ve Antivirüs yazılımıdır.

Çizge 5.2'de verilen Türkiye 'de kritik altyapılara yönelik gerçekleşen siber saldırı örneklerinde kullanılan siber saldırı yöntemlerinin kullanılma oranı grafikte gösterilmiştir.



Şekil 6.4. Türkiye'de Kritik Altyapılara Yönelik Gerçekleşen Siber Saldırı Türü Oranı

Şekilde görüldüğü gibi en çok kullanılan saldırı yöntemleri DDoS, Casus Yazılım, Black Door, Virüs olduğu tespit edilmiştir. DDoS ve Casus Yazılım yöntemlerinin ortak amacı sistemin çalışmasının engellenmesi ya da sisteminin yavaşlatarak, hizmetin engellenmesi hedeflenirken, kötü amaçlı yazılım türleri olan Black Door ve Virüs kişilerin izni olmadan bilgisayar sistemlerine sızmaktır. Bu iki saldırı yöntemine karşı kullanılacak korunma yöntemi en iyi Firewall, IDS /IP ve Antivirüs yazılımıdır.

Bu tezde siber güvenlik kavramı üzerinde durulmuş ve Türkiye'de ve dünyada gerçekleştirilen siber saldırılar incelenmiştir. Toplamda 45 adet saldırı seçilmiş ve siber saldırıların amaçları ve saldırı için kullanılan yöntemler incelenmiştir. Yapılan bu inceleme sonucunda en yaygın olarak kullanılan saldırı türlerinin hizmet durdurmaya ve verileri ele geçirmeye yönelik olduğu görülmüştür. Hizmet durdurma için genellikle DoS/DDoS saldırıları, verileri ele geçirmek için ise Casus ya da fidye yazılım kullanıldığı belirlenmiştir. Hizmet durdurma ve verileri ele geçirmeye yönelik olarak yapılan siber saldırılardan korunmak ve bunları önlemek amacıyla güncel bir antivirüs kullanımının şart olduğu açıktır. Yazılımsal ya da donanımsal bir güvenlik duvarı (firewall) kullanımı güvenliğimizi arttıracaktır. Bunların yanında saldırı tespit sistemi (IDS) ve saldırı engelleme sistemleri (IPS)'nin kullanımı da hizmet durdurma ve verileri ele geçirmeye yönelik olarak yapılan siber saldırıları engellemek için kullanılabilecek olan ağ güvenliğini arttırıcı unsurlardır.

KAYNAKLAR

Adams, M., & Makramalla, M. (2015). Cybersecurity Skills Training: An Attacker-Centric Gamified Approach. *Technology Innovation Management Review*, *5*(1).

Adır, A. E. (2019). Kurumlar İçin Siber Güvenlik Laboratuvarı Altyapısının Oluşturulması. Yüksek Lisans Tezi, KTO Karatay Üniversitesi, Fen Bilimleri Enstitüsü, Konya.

Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A Taxonomy of Cyber-Harms: Defining The Impacts of CyberAattacks and Understanding How They Propagate.Journal of Cybersecurity, 4(1), tyy006.

Akbaş, Y. (2022). Milli Denizaltı Yönetim Sistemi Müren'i ve Tübitak'ı Hedef Alan Siber Saldırı Tespit Edildi, https://www.donanimhaber.com/milli-denizalti-yonetim-sistemi-muren-ve-tubitak-a-siber-saldiri--151976 sitesinden 22.09.2022 tarihinde erişilmiştir.

Akbulut, B. (2017). Bilişim Alanında Suçlar, Ankara, Adalet Yayınevi.

Algaç, G. (2020). Siber Güvenlik Alanında Düzenlenen Uygulamalı Öğretici CTF Yarışmalarında Kullanılan Programlara Genel Bir Bakış. Yüksek Lisans Tezi, İnönü Üniversitesi, Fen Bilimleri Enstitüsü, Malatya.

Altun, F. (2022). Fahrettin Altun'dan Siber Saldırı Açıklaması, https://www.ensonhaber.com/gundem/fahrettin-altun-2022de-turkiyeye-53-bin-siber-saldiri-gerceklesti sitesinden 22.09.2022 tarihinde erişilmiştir.

Ashmore, William C., Impact of Alleged Russian Cyber Attacks, Baltic Security & Defence Review, Vol. 11, No. 1, 2014, pp. 4-40.

Aslay, F. (2017). Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi. International Journal of Multidisciplinary Studies and Innovative Technologies, 1(1), 24-28.

Aytekin, A. (2015). Türkiye'nin Siber Güvenlik Stratejisi ve Eylem Planının Değerlendirilmesi. Yüksek Lisans Tezi, Gazi Üniversitesi, Bilişim Enstitüsü, Ankara.

Ayvaz, T. (2022). Firewall Nedir?, https://www.mediaclick.com.tr/tr/blog/firewall-nedir sitesinden 09.10.2022 tarihinde erişilmiştir.

Balat, İ. (2018). Modern Şifreleme Yöntemleri (Simetrik & Asimetrik Şifreleme), https://www.kerteriz.net/modern-sifreleme-yontemleri-simetrik-asimetrik/amp/ sitesinden 07.11.2022 tarihinde erişilmiştir.

Baltazar, J., Costoya, J., Flores, R., The Heart of Koobface C&C and Social Network Propagation, Trend Micro Threat Research, (2009).

Bakrania, S. with H. Haider (2016). Safety, Security and Justice: Topic Guide. Birmingham, UK: GSDRC, University of Birmingham. https://gsdrc.org/topic-guides/safety-security-andjustice/themes/national-security-architectures/

BBCTurkish (2009). ABD ve G. Kore'de Siber Saldırı, https://www.bbc.co.uk/turkish/news/story/2009/07/printable/090708_cyber_attack.shtml sitesinden 06.07.2022 tarihinde erişilmiştir.

BBC, (2017). Fidye Yazılımı 'WannaCry' Türkiye Dahil 99 Ülkede Binlerce Bilgisayarı Etkiledi, https://www.bbc.com/turkce/39899848 sitesinden 06.07.2022 tarihinde erişilmiştir.

Benedikt, M. (Ed.). (1991). *Cyberspace: First Steps*. Mit Press.

Bıçakcı, S., Ergun, D., & Çelikpala, M. (2015). Türkiye'de Siber Güvenlik. Ekonomi ve Dış Politika Araştırma Merkezi (EDAM) Siber Politika Kağıtları Serisi, 1, 1-35.

Bitdefender, (2022). Antivirüs Nedir?, https://bitdefender.com.tr/antivirus-nedir/ sitesinden 09.10.2022 tarihinde erişilmiştir.

Bolubeyi, (2013). Şifre Saldırıları https://bolubeyi.net/sifre-saldirilari-password-attacks.html sitesinden 17.11.2022 tarihinde erişilmiştir

Cavelty, M. D. (2008). Cyber-Terror-Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. *Journal of Information Technology & Politics*, *4*(1), 19-36.

Canbek G., & Sağıroğlu Ş. (2006). Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri, Grafiker Yayıncılık, ISBN 975- 6355-26-3.

Canbek, G., ve Sağıroğlu, Ş. (2007). Çocukların ve Gençlerin Bilgisayar ve İnternet Güvenliği. Politeknik Dergisi, 10(1), 33.

Canbek, G., & Sağıroğlu, Ş. (2007). Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma. Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 22(1).

Cnbc, (2022). Cyberattack Hits Norway, Pro-Russian Hacker Group Suspected, https://www.cnbc.com/2022/06/30/cyberattack-hits-norway-pro-russian-hacker-group-suspected.html sitesinden 07.06.2022 tarihinde erişilmiştir.

Coveware (2020). Ransomware Attacks Fracture Between Enterprise and Ransomware-as-a-Service in Q2 as Demands Increase, https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report#1 sitesinden 15.05.2022 tarihinde erişilmiştir.

Cumhuriyet (2014). Boru Hattını Klavyeyle Patlattılar, https://www.cumhuriyet.com.tr/haber/boru-hattini-klavyeyle-patlattilar-161657 sitesinden 02.07.2022 tarihinde erişilmiştir.

Cummins, J., Diskin, P., Lau, S., ve Parlett, R., Steganography and Digital Watermarking, http://www.cs.bham.ac.uk/~mdr/teaching/modules03/security/students/ SS5/Steganography .pdf (21 Ağustos 2022).

CyberArts (2021). Dünyada İlk Siber Saldırıya Bağlı Ölüm, https://cyberartspro.com/saglik-sektorunde-siber-saldirilar/ sitesinden 06.07.2022 tarihinde erişilmiştir.

Çiftçi, H. (2018). Siber Zorbalık Davranışları ve Siber Mağduriyet Düzeylerinin Karşılaştırılması. *Anemon Muş Alparslan Üniversitesi Sosyal Bilimler Dergisi*, *6*(6), 887-897.

Tureng Sözlük. (2022). https://tureng.com/tr/turkce-ingilizce/cyberspace sitesine 12.04.2022 adresinden erişildi.

Çeliktaş, B. (2016, Mayıs). Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme. Yüksek Lisans Tezi, Karadeniz Teknik Üniversitesi, Sosyal Bilimler Enstitüsü (Trabzon).

Drozhzhin, A. (2014). Darkhotel: A Spy Campaign in Luxury Asian Hotels, https://www.kaspersky.com/blog/darkhotel-apt/6613/ sitesinden 23.05.2022 tarihinde erişilmiştir.

Edevlet, (2022). https://giris.turkiye.gov.tr/Giris/gir sitesinde 09.10.2022 tarihinde erişildi.

Ergüç, S. (2008). Türk Bankacılık Sisteminde İnternet Bankacılığı ile Yapılan Dolandırıcılıklar ve Bilişim Suçları Hukuku. Yüksek Lisans Tezi, Kadir Has Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul.

Geçmez, İ. (2019). Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçları (Tck m. 244). Yüksek Lisans Tezi, Marmara Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul.

Gustin, J., (October 15,2003). Cyber Terrorism, Marcel Dekker, 26- 27.

Güden, O. (2019). Ağ Güvenliği Nedir?, https://fordefence.com/saldiri-tespit-ve-onleme-sistemleri-ids-ips/ sitesinden 09.10.2022 tarihinde erişilmiştir.

Gül, A. (2016), Doğrudan / Dolaylı Bilişim Suçları, 1. Baskı, Seçkin Yayınevi, Ankara.

Gürkaynak, M., & İren, A. A. (2011). Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler. Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 16(2), 263-279.

Haberturk, (2020). Türkiye DDoS Saldırısı Altında! Garanti ve Türk Telekom'dan Açıklama Geldi, https://www.haberturk.com/son-dakika-garanti-ve-turk-telekom-na-siber-saldiri-aciklamamasi-haberler-2535014-teknoloji sitesinden 02.07.2022 tarihinde erişilmiştir.

Havelsan, (2018). Muddy Water (APT) Siber İstihbarat Saldırısı Hakkında Bilgilendirme, https://www.cybermagonline.com/konu-muddy-water-apt-siber-istihbarat-saldirisi-hakkinda-bilgilendirme sitesinden 02.07.2018 tarihinde erişilmiştir.

Havorth, J. (2022). Turkish Flight Operator Pegasus Airlines Suffers Data Breach, https://portswigger.net/daily-swig/turkish-flight-operator-pegasus-airlines-suffers-data-breach sitesinden 22.09.2022 tarihinde erişilmiştir.

Heavy, (2017). Petya/Notpetya Ransomware Attack: 5 Fast Facts You Need to Know, https://heavy.com/tech/2017/06/notpetya-petya-ransomware-attack-virus-patch-petrwap-victims/ sitesinden 09.10.2022 tarihinde erişilmiştir.

Hekim, H., & Başıbüyük, O. (2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi*, *4*(2), 135-158.

Heylighen, F., & Joslyn, C. (2001). Cybernetics and Second-Order Cybernetics. *Encyclopedia of Physical Science & Technology*, *4*, 155-170.

Holat, O. (2021). Yeni Medya ve Siber Savaş Kavramları Bağlamında Stuxnet Saldırısı Örneğinin İncelenmesi. Abant Kültürel Araştırmalar Dergisi, 6(11), 105-121.

Hootsuite, W. A. (2019). We Are Social, https://wearesocial.com/global-digital-report-2019 sitesinden 31.01.2019 tarihinde erişilmiştir.

Hürriyet, (2011). Yıllardır Süregelen Gerilim Savaşa Dönüşüyor, https://www.hurriyet.com.tr/gundem/yillardir-suregelen-gerilim-savasa-donusuyor 19161009 sitesinden 07.07.2022 tarihinde erişilmiştir.

Hürriyet, (2016). Ukrayna'da Elektrik Dağıtım Sistemi Siber Saldırıya Uğradı, https://www.hurriyet.com.tr/teknoloji/ukraynada-elektrik-dagitim-sistemi-siber-saldiriya-ugradi-40043686 sitesinden 06.07.2022 tarihinde erişilmiştir.

Hürriyet, (2017). Siber Saldırının Yeni Adı Petya, http://www.hurriyet.com.tr/siber-saldirinin-yeni-adi-petya-40503497 sitesinden 26.06.2017 tarihinde erişilmiştir.

Iraqi News Agency (2022). DMC: Cyber Attack Disrupts Turkish Airlines Website, https://ina.iq/eng/20884-dmc-cyber-attack-disrupts-turkish-airlines-website.html sitesinden 22.09.2022 tarihinde erişilmiştir.

Jerome, N. (2013). Application of the Maslow's Hierarchy of Need Theory; Impacts and Implications on Organizational Culture, Human Resource and Employee's Performance. *International journal of business and management invention*, 2(3), 39-45.

Ji, L. (2022). Investigation Report on New APT Organization MurenShark: Torpedoes Fired to Turkish Navy?, https://nsfocusglobal.com/investigation-report-on-new-apt-organization-murenshark-torpedoes-fired-to-turkish-navy-1/ sitesinden 09.10.2022 tarihinde erişilmiştir.

Junjie, W. (2018). Detection and Analysis of Web-Based Malware and Vulnerability. Doctoral Thesis, Nanyang Technological University. School of Computer Science and Engineering, Singapore.

Kara, İ. (2019). Truva atı zararlı yazılımlarına yaklaşım ve çözüm önerileri. *Bilgi Yönetimi*, *2*(1), 28-33.

Karaarslan Enis, Ağ Güvenlik Duvarı Çözümü Oluşturulurken Dikkat Edilmesi Gereken Hususlar, Akademik Bilişim 2003.

Karabacak, B. (2011). Kritik Altyapılar, Dünya ve Türkiye Özeti. BİLGEM, Cilt 3, Sayı 5(24).

Karakış, T. (2022). Ünlü Restoran Zincirine Siber Saldırı: Yarım Milyon Kişinin Verisi Çalındı!, https://shiftdelete.net/unlu-restoran-zincirine-siber-saldiri-yarim-milyon-kisinin-verisi-calindi sitesinden 02.07.2022 tarihinde erişilmiştir.

Karel (2019). Siber Saldırı: Nedir, Nasıl Yapılır, Türleri ve Nasıl Takip Edilir?, www.karel.com.tr/blog/siber-saldiri-nedir-turleri-nelerdir sitesinden 05.05.2022 tarihinde erişilmiştir.

Kaspersky (2019). Reklam Yazılımı Nedir?, https://www.kaspersky.com.tr/resourcecenter/threats/adware sitesinden 15.05.2022 tarihinde erişilmiştir.

Kaspersky (2020). Fidye Yazılımlarının Tanınması – Şifrelenmiş Truva Atlarından Farkı Nedir?, https://www.kaspersky.com.tr/resource-center/threats/ransomware sitesinden 15.05.2022 tarihinde erişilmiştir.

Kınay, H. (2012). Lise Öğrencilerinin Siber Zorbalık Duyarlılığının Riskli Davranış, Korumacı Davranış, Suça Maruziyet ve Tehlike Algısı İle İlişkisi ve Çeşitli Değişkenler Açısından İncelenmesi (Master's Thesis, Sakarya Üniversitesi).

Klimburg, A., & Tirmaa-Klaar, H. (2011). Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action Within the EU.

Kochetkova, K.(2016). İnterneti Nasıl Kırmazsınız?, https://www.kaspersky.com.tr/blog/attack-on-dyn-explained/2629/ sitesinden 23.05.2022 tarihinden erişilmiştir.

Kocamaz, C. (2009). Kimlik Hırsızlığına Karşı Web Tarayıcıların Kullanımı Kimlik Hırsızlığı , www.sayisaldelil.net sitesinden 16.05.2022 tarihinde erişilmiştir.

Koçoğlu, S.(2019). Bilişim Sistemine ve Sistemdeki Verilere Müdahale İle Bilişim Sistemi Aracılığıyla Haksız Çıkar Sağlama Suçları (TCK M. 244). Yüksek Lisans Tezi, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul.

Krämer, N. C. & Kappas, A., (Eds.). (2011). *Face-to-Face Communication Over the Internet: Emotions In A Web Of culture, Language, and Technology*. Cambridge University Press.

Kurnaz, İ. (2016). Siber Güvenlik ve İlintili Kavramsal Çerçeve. Siber Politikalar Dergisi, 1, (1). [Çevrimiçi]. http:// cyberpolitikjournal.org/wpcontent/uploads/2017/02/ Journal_Dergi_pdf.pdf (Erişim Tarihi: 10.07.2022).

Lakshmanan, R. (2022). PseudoManuscrypt Malware Spreading the Same Way as CryptBot Targets Koreans, https://thehackernews.com/2022/02/pseudomanuscrypt-malware-spreading-same.html sitesinden 07.07.2022 tarihinde erişilmiştir.

Lene Halsen, H. N. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, 53,1155–1175.

Malhotra, A. (2022). Iranian APT MuddyWater Targets Turkish Users Via Malicious PDFs, Executables, https://blog.talosintelligence.com/2022/01/iranian-apt-muddywater-targets-turkey.html sitesinden 31.01.2022 tarihinde erişilmiştir.

Marks A. (2007). Exploring Universities' Information Systems Security Awareness In A Changing Higher Education Environment: A Comparative Case Study Research. PhD thesis, University of Salford.

Medilife (2022). Siber Saldırganlar Türkiye'de 500 Bin Hastaya Ait 2,5 Milyon Kaydı Ele Geçirdi, https://www.medilife.com.tr/27-basin/37-bizden-haberler/3762-kamuoyuna-duyuru/ sitesinden 02.07.2022 tarihinde erişilmiştir.

Mitnick, K. (2006). *Aldatma Sanatı.* Ankara: Odtü.

M. Goodrich, R. T. (2010). *Introduction to Computer Security*. USA: Addison-Wesley Publishing Company.

Mohay, G., Collie, B., Vel, O., McKemmish, R., Anderson, A., (April 1, 2003). Computer and Intrusion Forensics, Artech House, 226.

Mukhtar, H., Salah, K., & Iraqi, Y. (2012, 09). Mitigation of DHCP Starvation Attack. *Computers & Electrical Engineering*, 1115-1128.

Nye, J. S. (2011). Nuclear Lessons For Cyber Security?. *Strategic Studies Quarterly*, *5*(4), 18-38.

Özavcı, F. (2013). Metasploit Framework Giriş Seviyesi Denetmen Rehberi, GamaSEC Bilgi Güvenliği Denetim ve Danışmanlık, S.1-251,Ankara.

Özdemir, Ö. N. (2020). DSA Şifreleme, https://www.sibervatan.org/makale/dsa-sifreleme/35 sitesinden 09.10.2022 tarihinde erişilmiştir.

Paulsen, C., McDuffie, E., Newhouse, W., & Toth, P. (2012). NICE: Creating A Cybersecurity Workforce and Aware Public. *IEEE Security & Privacy*, *10*(3), 76-79.

Peikari, C., Fogie, S.,(December 18, 2002). Maximum Wireless Security, Sams Publishing, 153, 164.

Polat, D. (2020). Nato'nun Yeni Operasyon Alanı: Siber Uzay. *Güvenlik Bilimleri Dergisi*, (International Security Congress Special Issue), 135-158.

Reis, A. R., Gülseçen, S., & Bayrakdar, B. (2010). Güvenli Internet Bankacılığı Eğitim Sistemi: GIBES. Akademik Bilişim Konferansı, 3.

Sağıroğlu, Ş., Alkan, M., & vd. (2018). Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık. Ankara: Grafiker Yayınları.

Sağlık Bakanlığı (2016). Sağlık Bakanlığı Hastanelerine Yönelik Siber Saldırı Girişimine İlişkin Basın Açıklaması, https://www.saglik.gov.tr/TR,3501/saglik-bakanligi-hastanelerine-yonelik-siber-saldiri-girisimine-iliskin-basin-aciklamasi-18052016.html sitesinden 02.07.2022 tarihinden erişilmiştir.

Sancar, G. (2019). ARP Spoofing Saldırısı, http://gsancar.com/arp-poisoning-ve-mitm-saldirisi/ sitesinden 09.10.2019 tarihinde erişilmiştir.

Savunmatr (Ocak, 2022). İrlanda Sağlık Sistemi Milyonlar Kaybetti, https://www.savunmatr.com/siber-guvenlik/irlanda-saglik-sistemi-milyonlarkaybettih16265 .html sitesinden 07.07.2022 tarihinde erişilmiştir.

Sertçelik, A. (2015). Siber Olaylar Ekseninde Siber Güvenliği Anlamak. Medeniyet Araştırmaları Dergisi, 2(3), 25-42.

Shafaq News (2022). Turkish Official Websites Hit By Cyber Attacks After Launching the Claw Lock Operation, https://shafaq.com/en/World/Turkish-official-websites-hit-by-cyber-attacks-after-launching-the-Claw-lock-operation sitesinden 22.09.2022 tarihinde erişilmiştir.

Siber Bülten, (2015). 8. Yılında Estonya Saldırılarına Çok Boyutlu Bir Bakış, https://siberbulten.com/siber-saldirilar-2/8-yilinda-estonya-saldirilarina-cok-boyutlu-birbakis/ sitesinden 26.06.2015 tarihinde erişilmiştir.

Siber Bülten, (2018). GitHub, Dev DDoS Saldırısını Geri Püskürttü,https://siberbulten.com/siber-guvenlik/github-dev-ddos-saldirisini-geri-puskurttu/ sitesinden 06.03.2018 tarihinde erişilmiştir.

Simmons, G. J. (1984). The Prisoners' Problem and the Subliminal Channel. In *Advances In Cryptology* (pp. 51-67). Springer, Boston, MA.

Singer W., P., & Friedman, A. (2015). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.

Skoudis, E., (November 7, 2003). Malware: Fighting Malicious Code, Prentice Hall PTR, 13, 96, 123-125, 149-151, 179.

SonDakika, (2021). Konya Büyükşehir Belediyesi'ne Siber Saldırı Şoku: 1 Milyon Kişiye Ait Bilgiler Çalındı, https://www.sondakika.com/haber/haber-konyabuyuksehirbelediyesine-siber-saldiri-soku-14122596/sitesinden 09.10.2022 tarihinde erişilmiştir.

Sputnik, (2021). Konya Büyükşehir Belediyesi'ne Siber Saldırı: 1 Milyon Kişinin Bilgileri Çalındı, https://tr.sputniknews.com/20210510/konya-buyuksehir-belediyesine-siber-saldiri-1-milyona-kisinin-bilgileri-calindi-1044463719.html sitesinden 02.07.2022 tarihinde erişilmiştir.

Şahinaslan, Ö. (2007). Bilgisayar Ağlarında Açık Kaynak Kodlu Güvenlik Yazılımları ile Anti-Spam Modülünün Geliştirilmesi. Yüksek Lisans Tezi, Maltepe Üniversitesi, Fen Bilimleri Enstitüsü.

Şenol, M. (2016). Siber Güçle Caydırıcılık Ama Nasıl?. Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 2(2), 10-17.

Şenol, M. (2012). Siber Savaş, Silahlı Kuvvetler Dergisi, Gnkur. ATASE Yayınları. Sayı:413, Ankara.

Şimşek, S. (2021). Kimlik Bilgileri Doldurma Saldırıları Nedir?, https://tr.linkedin.com/pulse/veri-tehlikesi-kimlik-bilgileri-doldurma-stuffing-simsek adresinden 24.05.2022 tarihinde erişilmiştir.

SCZTine, (2016). Virüs ve Solucan Arasındaki Ayrım Nedir?, https://www.sctzine.com/virus-ve-solucan-worm-arasindaki-ayrim-nedir/ sitesinden 15.05.2022 tarihinden erişilmiştir.

Shabtai, A., Moskovitch, R., Elovici, Y., Glezer, C. (2009). Detection of Malicious Code by Applying Machine Learning Classifiers On Static Features: A State-of-The-Art Survey. Information Security Technical Report, Vol. 14(1), pp. 16–29.

Shakarian P., Shakarian J. and Ruef A. (2013). Attacking Iranian Nuclear Facilities: Stuxnet in Introduction to cyber-warfare, Waltham, MA: Syngress-Elsevier, 224-235.

Şahinaslan, Ö. (2003). Siber Saldırılara Karşı Kurumsal Ağlarda Oluşan Güvenlik Sorunu ve Çözümü Üzerine Bir Çalışma (Basılmamış doktora tezi). 2-8. Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne.

TerraMedusa, (2013). Red October: 5 Senelik Tehdit, https://terramedusa.com/red-october-bes-senelik-tehdit/ sitesinden 07.05.2022 tarihinde erişilmiştir.

Tokmak, M., & Küçüksille, E. U. (2019). Kötü Amaçlı Windows Çalıştırılabilir Dosyalarının Derin Öğrenme İle Tespiti. Bilge International Journal of Science and Technology Research, 3(1), 67-76.

Tureng Sözlük. (2022). https://tureng.com/tr/turkce-ingilizce/cyberspace sitesine 12.04.2022 adresinden erişildi.

Turhost, (2021). Ransomware Nedir?, https://www.turhost.com/blog/ransomware-nedir/#serp sitesinden 15.05.2022 tarihinde erişilmiştir.

Turknetblog, (2022). Virüs Nedir? Antivirüs Programları Ne İşe Yarar?, https://turk.net/blog/virus-nedir-antivirus-programlari-ne-ise-yarar/ sitesinden 09.10.2022 tarihinde erişilmiştir.

Türk Dil Kurumu, (2021). https://sozluk.gov.tr/ sitesinde 15.12.2022 tarihinde erişildi.

T.C. Sağlık Bakanlığı, (2014). Siber Güvenlik, http://www.istanbulsaglik.gov.tr/, http://www.istanbulsaglik.gov.tr/w/anasayfalinkler/belge/siber_guvenlik_sunum.pdf sitesinde 15.12.2019 tarihinde erişildi.

UHDB. (2012). Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı. 9-47. T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı.

Ulaşanoğlu, M.E., Yılmaz, R.,Tekin M.A. (2010). Bilgi Güvenliği Riskler ve Öneriler. Bilgi Teknolojileri ve İletişim Kurumu Raporu. Ankara.

Uslu, T. (2007). İnternet Güvenliği ve Risk Yönetimi. Yüksek Lisans Tezi, İstanbul Kültür Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

Usta, O. (2021). Yemek Sepeti Saldırısı Hakkında Bilmeniz Gereken 5 Şey, https://siberbulten.com/siber-saldirilar-2/yemek-sepeti-saldirisi-hakkinda-bilmeniz-gereken-5-sey/ sitesinden 02.07.2021 tarihinde erişilmiştir.

Von Solms, R., & Van Niekerk, J. (2013). From Information Security to Cyber Security. *Computers & Security*, *38*, 97-102.

WayBackMachine, (2001). World - of – Hell, https://web.archive.org/web/20010721100203/http://world-of-hell.com/ sitesinden 07.06.2022 tarihinde erişilmiştir.

We are Social, (2022). Digital 2022: Another Year Of Bumper Growht, https://wearesocial.com/uk/digital-2022-another sitesinden 05.05.2022 tarihinde erişilmiştir.

Wikipedia, (2022). Confiker, https://pt.wikipedia.org/wiki/Conficker sitesinden 09.10.2022 tarihinde erişilmiştir.

WIRED, (2018). The Worst Cybersecurity Breaches of 2018 So Far, https://www.wired.com/story/2018-worst-hacks-so-far/ sitesinden 07.09.2018 tarihinde erişilmiştir.

Yazıcıoğlu, Y. (2006). Dialler, Keylogger Programları- İnternet Bankacılığı Dolandırıcılığı, Bilişim Hukuku, Dr. Mete Tevetoğlu, İstanbul, Kadir Has Üniversitesi Yayınları.

Ye, Y., Wang, D., Li, T., Ye, D., Jiang, Q. (2008). An Intelligent PE-Malware Detection System Based on Association Mining. Journal in Computer Virology, Vol. 4(4), pp. 323–334.

Yegin, F. (2015). DHCP Snooping ve Yapılandırma Adımları, https://www.cozumpark.com/dhcp-snooping-ve-yapilandirma-adimlari/ sitesinden 11.10.2015 tarihinde erişilmiştir.

Yener, Y. (2014). 8. yılında Estonya Saldırılarına Çok Boyutlu Bir Bakış, https://siberbulten.com/siber-saldirilar-2/8-yilinda-estonyasaldirilarina-cok-boyutlu-bir-bakis/ sitesinden 18.07.2022 tarihinde erişilmiştir.

Yönak, R. (2017). 2016'da Gerçekleştirilen Siber Saldırılar, https://www.bbc.com/turkce/haberler-38489376 sitesinden 03.01.2017 tarihinde erişilmiştir.

ÖZGEÇMİŞ

1990 yılında Manisa'nın Turgutlu ilçesinde doğdu. Lise öğrenimini Turgutlu ilçesi Zübeyde Hanım Anadolu Meslek Lisesi'nde tamamladı. 2010 yılında Adnan Menderes Üniversitesi Aydın Meslek Yüksekokulu Bilgisayar Teknoloji ve Programlama Bölümü'nden mezun olarak ön lisans eğitimini tamamladı. 2015 yılında ise lisans eğitimini Trakya Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümünde tamamladı. Çalışma hayatına 2013 yılında Trakya Üniversitesi Rektörlüğü'nde Bilgisayar İşletmeni olarak başlayan yazar halen bu görevi yürütmektedir.