# SİBER GÜVENLİK AÇISINDAN SİBER SALDIRI SENARYOLARININ İNCELENMESİ

Dilek Doğan
171402207

**YÜKSEK LİSANS TEZİ**
Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Yüksek Lisans Programı
Danışman: Dr. Öğr. Üyesi Ayşe Salman

İstanbul
T.C. Maltepe Üniversitesi
Lisansüstü Eğitim Enstitüsü
Eylül, 2021

# SİBER GÜVENLİK AÇISINDAN SİBER SALDIRI SENARYOLARININ İNCELENMESİ

Dilek Doğan
171402207
Orcid: 0000-0002-6489-1194

**YÜKSEK LİSANS TEZİ**
Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Yüksek Lisans Programı
Danışman: Dr. Öğr. Üyesi Ayşe Salman

İstanbul
T.C. Maltepe Üniversitesi
Lisansüstü Eğitim Enstitüsü
Eylül, 2021



# JÜRİ VE ENSTİTÜ ONAYI

Bu belge, Yükseköğretim Kurulutarafından 19.01.2021 tarihli *"Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge"* ile bildirilen 6689 Sayılı Kişisel Verilerin Korunması Kanunu kapsamında gizlenmiştir.

# ETİK İLKE VE KURALLARA UYUM BEYANI

Bu belge, Yükseköğretim Kurulutarafından 19.01.2021 tarihli *"Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge"* ile bildirilen 6689 Sayılı Kişisel Verilerin Korunması Kanunu kapsamında gizlenmiştir.

# TEŞEKKÜR

Tez yazma sürecimde motivasyon ve desteklerinden ötürü sevgili annem ve babam Seyhan-Hayati Doğan'a, değerli nişanlım Erdem Erkıran'a, abim kuzenim Sedat Sağlam ve teyzem ve eniştem Ceyhan-Fuat Sağlam'a, tüm ailem ve dostlarıma, bu süreçte birlikte çalışma fırsatı bulduğum ASG Grubu Sistem Yönetimi Müdürü Ali Samay ve ekip arkadaşlarım Kamil Çiçek, Özkan Türkmen, Selçuk Sadak, Yaşar Abravaya'ya tecrübelerini ve yönlendirmelerini eksik etmediklerinden ötürü değerli ekibime, gerek bir danışman gibi, gerekse bir abla gibi beni yönlendiren, bilgilendiren ve düşünen saygı değer Dr. Öğr. Gör. Danışmanım Ayşe Salman'a değerli desteklerinden ötürü teşekkür ederim.

Dilek Doğan

Eylül 2021

# ÖZ

## SİBER GÜVENLİK AÇISINDAN SİBER SALDIRI SENARYOLARININ İNCELENMESİ

Dilek Doğan
Yüksek Lisans Tezi
Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Yüksek Lisans Programı
Danışman: Dr. Öğr. Gör. Ayşe Salman
Maltepe Üniversitesi Lisansüstü Eğitim Enstitüsü, 2021

Çağımız artık teknolojinin rüzgarın yönüne geliştirilmesinden çok insan için teknolojinin geliştrilmesi bu sayede günlük yaşamı ve iş hayatını kolaylaştırma odaklı hale gelmiştir. İnsan hayatını kolaylaştıran teknolojik temelli gelişmeler onca olumlu katkısının yanında ciddi güvenlik kaygılarınıda beraberinde getirmiştir. Siber saldırı adını verdiğimiz bu yeni kavram ve doğurduğu sonuçlar tezimizin inşaasının temelini oluşturmuştur. Yapılan siber saldırıların insana, devletlere, şirketlere verdiği ekomik kayıplar ve psikolojik etkileri tezimizde irdelenmiştir. Artık hayatımızda yediden yetmişe herkesin kullandığı teklojik aletler ile kişisel bilgi ve belgelerin nasıl kolaylıkla el değiştirebildiği ve bunların sonuçlarının kişi ve kurumları maddi ve manevi açıdan ne kadar sarsıcı sonuçlar doğurabildiği gerçek ve sanal siber saldırı senaryoları ile gözler önüne serilmeye çalışılmıştır.

**Anahtar Sözcükler:** siber, saldırı, güvenlik, maddi, teknoloji.

# ABSTRACT

## INVESTIGATION OF CYBER ATTACK SCENARIOS IN CYBER SECURITY

Dilek Doğan
Master Thesis
Department of Computer Engineering
Computer Engineering Programme
Thesis Advisor: Asst. Prof. Ayşe Salman
Maltepe University Graduate School, 2021

In today's world, the goal of technology has shifted in order to meet people's needs, thus paving the way for a better and qualified life for humankind. As well as this led to positive technology-based advances that make our life easier, it also brought along cybersecurity concerns. This new concept that we called "cyber attack" and its consequences make the base of this thesis. In this paper, economic losses and psychological effects of syber attacks on people, governments and businesses are discussed. With real and virtual cyber attack scenarios, it is aimed to reveal how the technological tools used by everybody around the world can easily change hands and how they can result in disastrous material and moral consequences for individuals and businesses.

**Keywords:** cyber, attack, security, material, technology.

# İÇİNDEKİLER

JÜRİ VE ENSTİTÜ ONAYI ..... ii
ETİK İLKE VE KURALLARA UYUM BEYANI ..... iii
TEŞEKKÜR ..... iv
ÖZ ..... v
ABSTRACT ..... vi
İÇİNDEKİLER ..... vii
TABLOLAR LİSTESİ ..... viii
ŞEKİLLER LİSTESİ ..... ix
KISALTMALAR ..... xi
ÖZGEÇMİŞ ..... xiv
BÖLÜM 1. GİRİŞ ..... 1
1.1. Problem ..... 1
1.2. Amaç ..... 3
1.2. Önem ..... 3
1.4. Varsayımlar ..... 4
1.5. Sınırlıklar ..... 4
1.6. Tanımlar ..... 4
BÖLÜM 2. SİBER SALDIRI VE SİBER SALDIRI TÜRLERİ ..... 6
Siber Saldırı Nedir? ..... 6
Siber Saldırı Türleri Nelerdir? ..... 10
Hacker ve Cracker Nedir? ..... 27
Siber Saldırılara Karşı Güvenlik Tedbirleri ..... 28
BÖLÜM 3. GERÇEK VE SANAL SİBER SALDIRI SENARYOLARI VE OLASI ETKİLERİ ..... 31
BÖLÜM 4. SONUÇ VE DEĞERLENDİRME ..... 81
KAYNAKÇA ..... 84

# TABLOLAR LİSTESİ

Tablo 1. Sanal Abd Sağlık Sistemi Kuruluşu Yapısı..... 70

# ŞEKİLLER LİSTESİ

Şekil 1. OLTALAMA Kitinin Anatomisi ..... 21
Şekil 2 sosyal mühendislik saldırılarının yaşam döngüsü ..... 26
Şekil 3 Fiziksel uygulama senaryosu ..... 32
Şekil 4 Gerçek banka siber saldırı senaryosu ..... 33
Şekil 5 ziyaretçi defteri açıldığında otomatik yüklenen zararlı yazılım ..... 34
Şekil 6 sisteme zararlı yazılım sızması ..... 34
Şekil 7 Siber Saldırganın Yönetici Kullanıcı Hakkı Elde Etme Adımları ..... 35
Şekil 8 Wındows Güvenlik Kayıtları - Olay Özellikleri ..... 36
Şekil 9 Ortadaki Adam Saldırı mantığı ..... 37
Şekil 10 Lan'da ortadaki adam saldırı Senaryosu ..... 38
Şekil 11 LİNUX SUNUCUYA SIZMA SENARYOSU ..... 41
Şekil 12 Son Kullanıcı yapılan saldırı senaryosu ..... 45
Şekil 13 APT1 Saldırısının Sızdığı ülkeler ..... 46
Şekil 14 Sektörlere göre APT1 Saldırısının sızdığı firma sayısı ..... 47
Şekil 15 doğrulanmış apt1 sunucularının ülkelere göre dağılımı ..... 48
Şekil 16 Yemleme e-posta saldırı senaryosu ..... 50
Şekil 17 SAHTE DOĞRULAMA PAKETİ ..... 53
Şekil 18 wep yöntemiyle oluşturulan şifreyi kırma ..... 53
Şekil 19 SQL INjectıon saldırı senaryosu ..... 54
Şekil 20 XSS AÇIKLIĞI SALDIRI SENARYOSU ..... 55
Şekil 21 yetkilendirme açıklığı saldırı senaryosu ..... 56
Şekil 22 saldırı senaryoları için düşünce süreci ..... 61
Şekil 23 The sunday tımes gazetesi 25 temmuz 1999 moonlıgt maze siber saldırı haberi ..... 64
Şekil 24 SUNUCU ANAKARTLARA YERLEŞTİRİLEN ANAKART ..... 67
Şekil 25 ZARARLI MİKROÇİPİN ENTEGRE EDİLDİĞİ SUNUCU ANAKARTI ..... 68
Şekil 26 ZARARLI HALE GELMİŞ ANAKARTIN BULUNDUĞU SUNUCU ..... 69

Şekil 27 ÖZEL METNİN ŞİFRELENMESİ VE KOPYALANMASI ..... 74
Şekil 28 DICTIONARY SALDIRISI BAZINDA WORDLIST OLUŞTURMA ..... 74
Şekil 29 DICTIONARY SALDIRISI SONUCU ..... 75
Şekil 30 ZARARLI OLUŞTURULMASI ..... 76
Şekil 31 VIRUSTOTAL TESTİ ..... 77
Şekil 32 AĞA BAĞLI CİHAZLARIN TARANMASI VE WINDOWS ESET INTERNET SECURITY'E TAKILMASI ..... 77
Şekil 33 SIZMA KONFİGÜRASYONLARI ..... 78
Şekil 34 ANDROID CİHAZDA ARKA KAMERADAN GÖRÜNTÜ ALINMASI ..... 79

# KISALTMALAR

**ABD** : Amerika Birleşik Devletleri

**AIDS** : Kazanılmış Bağışıklık Yetersizliği Sendromu - Acquired Immune Deficiency Syndrome

**APT** : Gelişmiş Sürekli Tehdit - Advanced Persistent Threat

**AR-GE** : Araştırma - Geliştirme

**AWS** : Amazon Web Servisleri - Amazon Web Services

**BT** : Bilişim Teknolojileri

**BYOD** : Kendi Cihazınızı Getirin - Bring Your Own Device

**CGI** : Common Gateway Interface - Ortak Ağ Geçidi Arayüzü

**CIA** : Merkezî İstihbarat Teşkilatı - Central Intelligence Agency

**CPU** : Merkezi İşlem Birimi - Central Processing Unit

**DDOS** : Dağıtık Hizmet Engelleme - Distributed Denial of Service

**DR** : Doktor

**DWVA** : Düşük Düzey KorunmasızYazılım Test Wep Uygulaması - Damn Vulnerable Web Application

**EFT** : Elektronik Fon Transferi

**E-POSTA** : Elektronik Posta - Electronic Mail

**E-TİCARET** : Elektronik Ticaret

**FBI** : Federal Soruşturma Bürosu - Federal Bureau of Investigation

**FOIA** : Bilgi Edinme Özgürlüğü Yasası - Freedom of Information Act

**FTP** : Dosya Transfer Protokolü - File Transfer Protocol

**HTTP** : Hiper Metin Transfer Protokolü - Hyper Text Transfer Protocol

**IDS** : Saldırı Tespit Sistemleri - Intrusion Detection Systems

**IP** : İnternet Protokolü - Internet Protocol

**IPS** : Saldırı Önleme Sistemleri - Intrusion Prevention Systems

**ISP** : İnternet Servis Sağlayıcı - Internet Service Provider

**IT** : Bilişim Teknolojileri - Information Technology

**LAN** : Yerel Alan Ağı

**MFA** : Çok Faktörlü Kimlik Doğrulama - Multi Factor Authentication

**MITM** : Ortadaki Adam Saldırısı - Man In The Middle Attack

**MM** : Makers Mark

**NASA** : Ulusal Havacılık ve Uzay Dairesi - National Aeronautics and Space Administration

**NATO** : Kuzey Atlantik Antlaşması Örgütü - North Atlantic Treaty Organization

| | |
|---|---|
| **NSA** | : Ulusal Güvenlik Ajansı - The National Security Agency |
| **PHI** | : Kişisel Sağlık Bilgileri - Personal Health Information |
| **RAM** | : Rastgele Erişimli Hafıza - Random Access Memory |
| **SCADA** | : Merkezi Denetleme Kontrol ve Veri Toplama - Supervisory Control and Data Acquisition |
| **SOME** | : Siber Olaylara Müdahale Ekibi |
| **SPAM E-POSTA** | : İstenmeyen Elektronik Posta |
| **T.D.K.** | : Türk Dil Kurumu |
| **TELNET** | : İletişim Ağı - Telecommunication Network |
| **TGT** | : Bilet Sağlayan Bilet - Ticket Granting Ticket |
| **US-CERT** | : Amerika Birleşik Devletleri Bilgisayar Acil Durum Hazırlık Ekibi - United States Computer Emergency Readiness Team |
| **WEP** | : Kabloluya Eşdeğer Gizlilik - Wired Equivalent Privacy |
| **WPA** | : Kablosuz Korumalı Erişim - Wi-Fi Protected Access |
| **WPA2** | : Kablosuz Korumalı Erişim 2 - Wi-Fi Protected Access 2 |

# ÖZGEÇMİŞ

**Dilek Doğan**

**Bilgisayar Mühendisliği Anabilim Dalı**

**Eğitim**

| *Derece* | *Yıl* | *Üniversite, Enstitü, Anabilim/Anasanat Dalı* |
|---|---|---|
| Y.Ls. | 2018 – Devam Ediyor | Maltepe Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı |
| Ls. | 2014-2017 | Maltepe Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, Bilgisayar Mühendisliği Anabilim Dalı |
| Ön Ls. | 2012-2014 | Kırklareli Üniversitesi, Pınarhisar Meslek Yüksekokulu Bilgisayar Programcılığı |
| Lise | 2008-2012 | Mehmet Salih Bal Ticaret Meslek Lisesi, Web Tasarım ve Programlama Bölümü |

**İş/İstihdam**

| *Yıl* | *Görev* |
|---|---|
| *2021 – Devam Ediyor* | Koç Sistem Bilgi Teknolojisi ve Hizmetleri<br>SOC Uzmanı, Tehdit İzleme Analisti |
| *2020 – 2021* | Alternatif Bank – Alternatif Yatırım Menkul Değerler<br>Bilgi Teknolojileri Uzmanı |
| *2018 – 2020* | Acıbadem Sağlık Grubu<br>Sistem Yönetimi ve Güvenliği Uzman Yardımcısı |

**Mesleki Birlik/Dernek Üyelikleri**

| *Yıl* | *Kurum* |
|---|---|
| 2020 - | Üye: MSHOWTO Bilişim Topluluğu |

**Yayınlar ve Diğer Bilimsel/Sanatsal Faaliyetler**

www.mshowto.org/author/dilekdogan

# BÖLÜM 1. GİRİŞ

Bu bölümde, araştırmanın kimlik bilgilerinden olan problem, amaç, önem, varsayımlar, sınırlıklar ve tanımlara yer verilmiştir.

## 1.1. Problem

Siber saldırı, bir veya daha fazla bilgisayarı tek veya birden çok bilgisayara veya ağa karşı kullanan siber suçlular tarafından başlatılan bir saldırıdır. Siber saldırı, bilgisayarları kötü amaçlı olarak devre dışı bırakabilir, veri çalabilir veya ihlal edilen bir bilgisayarı diğer saldırılar için başlangıç noktası olarak kullanabilir. Siber suçlular, diğer yöntemlerin yanı sıra kötü amaçlı yazılım, kimlik avı, fidye yazılımı, hizmet reddi de dahil olmak üzere bir siber saldırı başlatmak için çeşitli yöntemler kullanır.

Yapılan bu siber saldırılar ile su ve kanalizasyon sistemlerine zarar görebilir ve yanlış yönetilebilir, ulaştırma altyapısına yapılan saldırı ile ulaşım sistemleri felç olabilir ve tüm telekomünikasyon sistemleri yanlış yönlendirilerek iletişim ve ekonomik altyapı engellenebilir. Yangın sistemlerine saldırı ise ciddi birçok soruna yol açabilir. Sürekli olarak sanayinin ocaklarını açık tutmak yangın felaketine neden olabilir ve bu nedenden dolayı binlerce can kaybı yaşanabilir. Nükleer sistemlere saldırı hepsinden daha da vahim ve geri dönülemez sonuçlara neden olabilir. Önemli atom kodlarının ve bilgilerinin kopyalanması ulusal ve küresel düzeyde ciddi bir felaketle sonuçlanabilir. Kişileri veya kitlesel bir nüfusu şiddetli bir şekilde etkilemek için kullanıcının veya tüm kuruluşların bilgilerini izinsiz kopyalamak rahatsız edici sonuçlara neden olabilir.

Siber saldırı ile yapılan dolandırıcılık maddi kayıplara yol açar ama esas zararı ise çalınmış olan verilerin özellikle Karanlık Web'de satılması bilgisayar korsanları için ve diğer üçüncü şahıslar için çok daha değerli olabilir. Fikri mülkiyet hırsızlığı kişilere ya da kuruluşlara önemli oranda zarar verebilir ve durumda şirketler yıllarca çabalayıp geliştirdiklerini kaybeder ve ticari sırlara veya telif hakkıyla korunan malzemelere Ar-Ge yatırımlarını ve rekabet avantajlarını kaybetmelerine neden olur.

Her kuruluş için, sızmanın zamanlaması ve süresi, faaliyet gösterdiği sektöre bağlı olarak bir sızmanın etkisi bakımından benzersizdir. Örneğin, bir veri ihlalinin finans sektörü için, örneğin imalattan daha belirgin sonuçları olabilir.

Müşteri ve paydaş güven kaybı, siber saldırının en zararlı etkisi olabilir, çünkü firmaların müşterilerin verilerini koruyamazsa, söz konusu şirketle bir daha iş yapmamayı tercih edebilir. Bu, doğrudan iş kaybına ve inşa etmek için çok çalıştığınız markanın devalüasyonuna dönüşebilir. Şirketin, tedarikçileri ve yatırımcıları çekme yeteneğini de olumsuz yönde etkileyebilir.

Siber saldırıların sonucunda, kişilerin hayatını tehdit etmeye, kopyalanan kişisel bilgileri kullanarak psikolojik baskı yoluyla depresyona girmelerine veya günlük faaliyetlerin aksamasına neden olabilir.

Siber saldırıların kamu, hükümet ve diğer akademik disiplinler için sahip olabileceği çoklu zararların anlaşılması açısından tezimizde bu zararların değerlendirilmesi yapılmıştır.

Fiziksel ve dijital açıdan bakıldığında can kaybı veya altyapıya zarar verilirken, ekonomik açıdan hisse senedi fiyatındaki düşüş, yasal para cezaları veya azalan kar gibi etkiler siber saldırıların olası sonuçları olarak karşımıza çıkabilir.

Psikolojik açıdan etkileri gözetildiğinde ise depresif, utanmış veya kafası karışmış bireyler yaratma gibi etkileri olabilir. İtibar açısından bakıldığında ise önemli personel kaybı, müşterilerle sorunlu ilişkilere neden olma ve yoğun medya baskısına maruz kalma gibi etkilere neden olabilir.

Siber saldırıları sosyal ve toplumsal açıdan değerlendirdiğimizde, üst düzey bir olaydan etkilenen kuruluşlarda kilit hizmetler, olumsuz bir teknoloji algısı veya iç moralin düşmesi gibi günlük iş ve yaşam döngüsünde bozulma riski doğurabilir.

Birçok başarılı siber saldırı, siber saldırılardan etkilenme biçimlerini anlamayan firmaların eyleme geçmemesi nedeniyle uygun bir şekilde ele alınmamış olan bilinen güvenlik açıklarının istismarına dayanmaktadır.

Bir siber saldırının bir işletmeyi ve üçüncü tarafları etkileyebileceği birçok farklı yolun ayrıntılı bir dökümünü sağlayarak, yönetim kurulu üyelerine ve diğer üst düzey personele, kuruluşlarının tehditlerini göz önüne alırken siber saldırıların doğrudan ve

dolaylı zararlarını daha iyi anlamalarını sağlar. Bu aynı zamanda diğer kuruluşlar ve hatta hükümetler veya kritik ulusal altyapıyı yönetenler için de kendilerini toparlayıp önlem alabilmeleri için geçerlidir.

### 1.2. Amaç

Bu araştırmanın temel amacı, yaşanmış veya sanal siber saldırı senaryolarını değerlendirerek kurumların veya kişilerin doğacak zararlar konusunda farkındalığının arttırılarak durumun ciddiyetine binayen siber güvenlik önlemlerini arttırmaları gerekirse profesyonel uzmanlarca yardım almaları ve gerekli güvenlik yazılımlarını kullanmaları ve bunları güncel tutmaları amaçlanmıştır. Bunun için aşağıdaki aşamalar hakkında farkındalık yaratılmaya çalışılmıştır.

- Siber saldırı kavramı nedir?
- Siber saldırılar hangi amaçlarla düzenlenir?
- Siber saldırı sonucunda kişisel zararlar hangi boyutlara ulaşabilir?
- Siber saldırı sonucunda kurumsal zararlar hangi boyutlara ulaşabilir?
- Siber saldırı sonucunda devletler ve küresel anlamda oluşabilecek zararlar hangi boyutlara ulaşabilir?
- Siber saldırı senaryolarını değerlendirerek alınacak önlemler nelerdir?
- Siber saldırı sonucunda oluşabilcek zararlar daha doğmadan farkındalık yaratılarak engellenebilir mi?
- Türkiye'de ve dünyada yaşanan siber saldırıların bilişim teknolojilerinin gelişimine katkıları ne yönde olmuştur?
- Anlık saldırılar ve zamana yayılan saldırıların kullandıkları yöntem ve amaçlarında görülen farklılıklar nelerdir?

### 1.2. Önem

Siber saldırıların kişisel veya kurumsal anlamda yeterince önemsenmemesi dolayısı ile yoğun bir kaygı duyulmadığı için kişiler ve kurumlar bu saldırılara daha açık bir halde sanal dünyada savunmasız veya yeterince savunma önlemleri almadan yer almaktadır. Sanal dünyadaki bilgi ve belgelerin yeterince korunmadan dolaşıyor olması beraberinde ciddi siber güvenlik sorunları doğurmakta, izinsiz kopyalanan bu veriler kurumları ve şahısları dönüşü olmayan sonuçlarla karşı karşıya bırakmaktadır. Bu

araştırmamızda saldırı senaryoları incelenerek doğan zararlar gösterilmiş ve konuya ciddiyetle yaklaşılması gerektiğinin önemi bir kez daha vurgulanmıştır.

### 1.4. Varsayımlar

Bu araştırmamızda kurumların, kişilerin ve kamu kuruluşların siber saldırılardan korunmak için yeterli siber güvenlik önlemleri almadığı, siber güvenlik yazılımlarını güncel tutmadığı veya siber güvenlik kavramını önemsemediği varsayılmıştır. Bu sayede kurbanların siber saldırıya daha açık halde oldukları varsayımıyla uğradıkları zararların normalden daha ciddi sonuçlar doğurduğu varsayımıyla hareket edilmiştir.

### 1.5. Sınırlıklar

Bu araştırmada yapılan bazı siber saldırıların manevi boyutlarının etkileri gözle görülür bir şekilde ortaya konulamayacağı için genel hatlarıyla yorumlanmıştır.

Bazı siber saldırılarda ise olay tam olarak aydınlatılmadığı için ortaya çıkan maddi ve manevi boyutlar tam olarak ortaya konulamamaktadır.

Yine bazı siber saldırların yıllarca düzenlenmiş olmasından kaynaklı sonuçlarınında kendini uzun yıllarda gösterebilme sonucu doğduğundan dolayı siber güvenlik açısından doğacak sıkıntılar tam olarak tanımlanamamış ve sızıntıların hepsi tamamen keşfedilemediğinden dolayı alınabilcek önlemler tam olarak anlamlandırılamamış olabilir.

### 1.6. Tanımlar

**Siber Saldırı:** Siber saldırı, herhangi bir bilgisayardan ya da birden fazla bilgisayardan kablolu veya kablosuz ağ üzerinden veri kopyalama, değiştirme ve silme gibi işlemler için karşı tarafa bilinçli olarak gerçekleştirilen her türlü iş ve eylemlerin bütününe verilen isimdir.

**Siber Güvenlik:** Siber güvenlik, sistemleri, ağları, programları, cihazları ve verileri siber saldırılara karşı korumak için teknolojilerin, süreçlerin ve kontrollerin uygulanmasıdır.

**Siber Saldırı Senaryosu:** Bir sanal sadırının adım adım uygulama aşamaları ve sonuçlarının adım adım izlenmesidir.

**Hacker (Kırıcı):** Özelde, bilgisayar ve bilgisayar ağları gibi sistemlerin içsel işleyişlerinin derin bilgisine sahip olmaktan zevk duyan kişi (ERİŞ, 2009)

**Cracker (Çökertici):** Bir sistemde güvenliği kıran kişi (ERİŞ, 2009)

**Log:** Meydana gelen olayların ve hareketlerin kayıt altına alındığı dosyalardır**.** (wmaraci.com, 2020)

**Ransomware (Ağ Fidye Yazılımı): B**ir miktar fidye ödenene kadar bir bilgisayar sistemine erişimi engellemek için tasarlanmış bir tür kötü amaçlı yazılımdır.

**Trojan:** Kendini meşru bir yazılım gibi göstermeye çalışarak sisteme kullanıcı onayıyla sızan, kötü amaçlı bir yazılımdır.

# BÖLÜM 2. SİBER SALDIRI VE SİBER SALDIRI TÜRLERİ

Çağımızın getirdiği baş döndürücü teknolojik yenilikler sayesinde hayatımıza bir çok yeni kavramlar girdi. Bunlardan sıklıkla duyduğumuz siber saldırı, siber savaş, hacker, cracker gibi terimleri ve artık yaşanan siber saldırılara karşı alınabilecek bireysel ve kurumsal güvenlik önlemlerini ele alacağız.

**Siber Saldırı Nedir?**

Siber terimi sibernetik kelimesinden gelmektedir. 1958 yılında makineler ve canlılar arasındaki iletişim üzerine araştırmalar yapan Louis Couffignal tarafından kurulan Sibernetik bilimini temel almaktadır. Siber saldırı, kişilik haklarına da bir saldırı niteliği taşımaktadır. Normal hayattaki taciz, tehdit ve şantaj gibi durumların dijital ortamda şahsi bilgilere saldırarak gerçekleştirilmesidir. Bu tür saldırılara, sanal ortamlarda daha fazla bulunmalarından dolayı çocuklar ve gençler daha çok maruz kalmaktadır. (Taşdöğen, 2019)

Siber saldırı, herhangi bir bilgisayardan ya da birden fazla bilgisayardan kablolu veya kablosuz ağ üzerinden veri kopyalama, değiştirme ve silme gibi işlemler için karşı tarafa bilinçli olarak gerçekleştirilen her türlü iş ve eylemlerin bütününe verilen isimdir. Kötü amaçlı yapılan bu saldırılar bazen internet sitelerine erişimi engellemek ve yavaşlatmak amacı da güdebilir.

Son dönemde siber saldırıları yapan kişiler örgütlü hale gelerek kendilerine buldukları bir isim çatısı altında örgütlenerek birlikte hareket etmeye başlamışlardır. Bu eğilim dünya genelinde artmakta bu da saldırıya uğrayan kişi ya da kurumların güvenlik önlemlerini oldukça zorlayabilmektedir. Yapılan örgütlü saldırılar beraberinde çoklu saldırıları getirdiği için aynı anda büyük grupların saldırılarını önlemek bir hayli zor olmaktadır.

Siber saldırılar devletler arası boyuta ulaştığında ise "Siber Savaş" olarakta adlandırılmaktadır. Siber savaşlarda genelde esas amaç devlet kurumlarına saldırarak iş göremez hale getirip karşı devleti itibarsızlaştırma çabası ya da gizli bilgi ile belgeleri sızdırmak üzere odaklanmıştır. Oldukça büyük maddi kayıplara neden olabilmektedir. Devletler çağımıza ayak uydurarak siber saldırılara karşı kendi siber güvenlik uzmanlarından oluşan birimleri ile gelmesi muhtemel saldırılara karşı önlem almaktadırlar.

Siber savaş, "Aynı saldırıların ülke veya ülkelere yönelik yapılmasıdır" . Siber savaşta hedef ülkelerin güvenlik, sağlık, enerji, haberleşme, su ve kanalizasyon, bankacılık ve kamu hizmetleri gibi kritik altyapıları saldırı alanı olarak seçilmektedir. (Yılmaz & Sağıroğlu, 2013)

Direk hedef gözeten siber saldırıların yanında kripto virüsleri gibi hedef gözetmeden de saldırı düzenleyebilen siber saldırıları tipleri vardır. Siber saldırı süreçlerini üç ana başlıkta incelemek mümkündür.

1. Tarama, bilgi toplama ve keşif
2. Erişim izni sağlamakx ve istismar etmek
3. Servis dışı bırakma saldırıları

İlk aşama olan keşif aşamasında siber saldırganların genel olarak amaçladığı nokta, hedef sistemler hakkında detaylı bilgi toplamak ve topladıkları bu bilgiler sayesinde ikinci aşamaya geçmek adına ön hazırlık amacıyla kullanırlar. Kullanıcının kullandığı sistemin zafiyetlerinin bulunması, sisteme bağlantı hakkı elde edebilmek için sahip olunması gereken kullanıcı haklarının tespit edilmesi, hedeflenen işletim sistemlerinin tespiti, güvenlik duvarı cihazları, IDS, IPS gibi güvenlik amaçlı kullanılan saldırı engelleme sistemleri ve benzeri güvenlik yazılımlarını saf dışı bırakabilmek için gerekli olan bütün verilerin toplanması sağlanır. Eğer ki hedef kurum, kuruluş ya da KOBİ ise, bilgi toplama aşamasında özellikle kolay hedef olarak gözüken çalışanlar üzerinde yoğunlaşılır. Özellikle sanal korsanlar, kurumlarda çalışan kişilerin Facebook, LinkedIn, Instagram ve Twitter benzeri sosyal medya hesaplarında var olan tüm kişisel bilgilerin bir kopyasını alarak, bu bilgileri kurumsal bilgileri elde edebilmek için ya da kişisel bilgilerini izinsiz erişim hakkına sahip olarak kullanabilmektedirler.

Kullanıcıya yapılan bilgi toplama saldırılarından sonra elde edilen bu bilgilerin kullanıldığı erişim elde etme aşamasına geçilir. Erişim elde etme aşamasında ise izinsiz edinilen tüm bilgiler kullanılarak saldırı düzenlenecek olan hedef sistemlere veya kişilere zararlı içeriğe sahip dosyalar, kötü niyetli kod parçacıkları veya kötü niyetli elektronik postalar gönderilerek sistem üzerinde yetkisiz erişim elde etmeye çalışılmaktadır. Maalesef ki zararlı yazılım bulaşan kişi ya da kurum bilgisayarı bulaşanın farkında değilse siber saldırganların amaçlarına kurban olabilir ve bunun sonucunda sistemlerine erişim için kişilerden kopyalanılan parola vb. bilgiler kullanılabilmektedir. Kullandığımız bilişim teknolojileri varlıklarının (IT) zafiyetleri bu aşamada kullanılan en önemli açıkları teşkil etmektedir. Ayarlamaları doğru olarak yapılandırılamamış bir güvenlik duvarı, antivirüs programı, saldırı önleme sistemi (IPS), saldırı tespit sistemi (IDS) gibi sistem güvenlik programlarını algılayarak bu cihazlar aracı olarak kullanıp işletim sistemlerinin açık noktalarını kullanarakta sisteminize yetkisiz erişim sağlama imkanını bulabilir.

Siber saldırganların sıklıkla kullandığı bir başka saldırı türü ise servis dışı bırakma diye adlandırdığımız DDoS saldırı türüdür. Bu şekilde yapılan saldırılar sonucunda kurumların bağlı olduğu tüm sunucularını ve internet bağlantısını kesmek kaydı ile dış dünya erişiminizin kopmasına ve iş yapamaz duruma gelmenize neden olabilmektedir. İnternetin iş hayatına etkin bir şekilde girmesiyle e-ticaret gibi tamamen sanal alandaki müşterilere hitap eden ve gelirlerini oluşturan şirketler için DDOS saldırıları oldukça önemli tehdit düzeyine sahiptir ve maddi açıdan şirketlere öngörülemez zararlar verebilecek kadar ağır sonuçlar oluşturulabilmektedir.

Siber saldırganlar kullanıcılara, kurum ve kuruluşlara aşağıda belirtildiği gibi zararlar verebilirler.

1. Müşterilerin kullandığı sistemin güvenlik duvarını atlatarak sisteme sızabilir ve müşteri verilerini kopyalayabilirler.
2. Kullanıcıların sahip olduğu bilişim teknolojileri (IT) varlıkları üzerinde saklanan müşterilerin bilgileri ve ticari kayıtlar gibi bilgileri kriptolayarak kullanılmaz hale getirip, bu kriptonun çözülmesi için karşılığında fidye isteyebilirler.
3. Kameranızı veya mikrofon sizden habersiz açarak, ortam kaydı alabilir ve bulunan ortamın dinlenilmesi ile elde ettikleri verileri internetteki üçüncü

şahıslara çıkar karşılığı ya da başka amaçla aktarabileceği gibi şantaj amacı ile de değerlendirebilirler.

4. Kullandığınız ağınıza sızarak bilgilerinizi ve dosyalarınızı izinsiz çoğaltatıp kullanabilir ve rakip firmalara satabilirler.
5. Var olan sistemlerinizi çalışamaz bir hale getirmek kaydıyla kurumun işlerliğini durdurabilir, sekteye uğratabilirler veya itibar kaybı sağlayabilirler.
6. DDoS yani hizmet dışı bırakma saldırıları düzenleyerek kurum itibarına ulusal veya uluslararası arenada zarar verebilecekleri gibi maddi açıdan geri dönülemeyecek büyüklükte zararlara yol açabilme imkanına sahip olabilirler.
7. SPAM e-postaları göndererek sisteminizde bulunan dosyalarınıza zararlı kodlar aracılığı ile virüs bulaştırabilirler.
8. Farkında olmadan gezdiğiniz siteler veya programların kaydını tutarak kredi kartı ile bankacılık bilgileriniz ve parolanız gibi gizliliği yüksek derecede önem arzeden bilgileri elde ederek kişisel veya kurumsal hesaplarınızı boşaltma imkanı bulabilirler.
9. Kişisel ya da şirkete ait olan bilgisayarları başka şirketlere veya devletlere saldırı düzenlemek için kullanabilirler.
10. Kişisel ya da şirkete ait olan bilgisayarların işlemcinin (CPU) ve geçici belleğin (RAM) sahip olduğu potansiyelleri, Bitcoin ve buna benzer dijital para birimleri üretebilmek için madencilik amacıyla değerlendirebilirler.

Siber saldırı, "hedef seçilen şahıs, şirket, kurum, örgüt, gibi yapıların bilgi sistemlerine veya iletişim altyapılarına yapılan planlı ve koordineli saldırılardır". (Yılmaz & Sağıroğlu, 2013)

Siber saldırıyı genel olarak bilgi ve iletişim sistemlerini kullanan elektronik araçların, bilgisayar yazılımlarının veya başka elektronik iletişim modellerinin kullanılması sayesinde ulusal ve ya uluslararası çıkarların dezenforme edilmesini amaçlayan kişisel ve gurup olarak bir yöne doğru kanalize edilmiş belli bir amaç doğrultusundaki eylem ve etkinlikler olarak tanımlayabiliriz.

Çağımızda yaygınlaşan internet kullanım oranları ile birlikte siber saldırı, başka bir söylemle düzenlenen sanal saldırı olayları da sürekli artış göstermektedir.

Siber saldırılar ve siber güvenliğin önemi, bilişim sistemlerinin insan hayatındaki yeri arttıkça yani IP (internet protokolü) adresi alan cihazların sayısı arttıkça, her geçen gün artmaktadır. (Özbay, 2015)

Güvenlik uzmanları ile bilgisayar korsanları arasında devam eden mücadeleler sayesinde sistemlerin daha da güvenli hale geldiği savunulabilir. Bu yarışın sonucu olarak da ortaya gelişmiş siber saldırı olarak adlandırılan, çok daha karışık ve gelişmiş tekniklerin kullanıldığı ve uzun çalışmalar sonucunda ve belirli bir amaç doğrultusunda tecrübeli bilgisayar korsanları tarafından yapılan hatta devletlerin desteklediği bilinen ve/veya düşünülen saldırılar ortaya çıkmıştır. Bu gelişmiş saldırı türü APT (Advanced Persistent Threat) olarak adlandırılmıştır. (Özbay, 2015)

Genç bilgisayar korsanları ve küçük ölçekli suçlulardan ziyade karmaşık (sofistike) saldırı yapabilen tecrübeli bilgisayar korsanları ve devlet destekli saldırganlar devletler ve işletmeler için en çok tehlike arz eden tehditlerdir. Bu saldırganlar öncelikle kurumlardaki bilgileri çalmaya ve bireyleri ya da işletmeleri dolandırmaya odaklanmaktadır. APT saldırısı, genellikle devlet destekli olup gelişmiş yöntemlerle organizasyonlara sızarak haftalarca, aylarca hatta yıllarca bu organizasyonların tespit etmesine karşı saklanarak, bilgi kaçırmak için yapılan saldırıdır. (Özbay, 2015)

APT hedefi net olarak belirlenmiş, ileri seviyede ve uzun süreli tehditler içeren, siber savaşlarda kullanılmak üzere geliştirilmiş zararlı saldırı yazılımlarıdır. APT'ler genellikle devletlerin kritik altyapılarını hedeflemektedir. (Özbay, 2015)

**Siber Saldırı Türleri Nelerdir?**

Siber saldırı çeşitli yollarla yapılabilir. Örneğin saldırı yapılacak bilgisayarın, kişinin ya da kurumun şifre bilgileri ele geçirmek sureti ile yapılabilir. Şifre bilgileri alındıktan sonra saldırı işlemi için gerekli hazırlıklar yapılır. Devamında da virüs içeren elektronik mesajlar, bildirimler ya da içerikler gönderilerek sanal saldırı işlemi yapılmaktadır. Bu tarz saldırı yönteminde, saldırı öncesi bir takım hazırlık ve bilgi toplama işlemi yapıldıktan sonra siber saldırıya işlemi başlatılır. İkinci bir siber saldırı yöntemi ise siber ortamdan bireye psikolojik baskı oluşturarak sanal zorbalık yapmak kaydıyla onu toplum önünde küçük düşürecek bir şekilde yapılan saldırı yöntemidir.

İkinci saldırı yönteminde sonuçlar maddi kayıplardan öteye kişinin hayatını sonlandırma teşebbüslerine varan ağır sonuçlara kadar gidebilmektedir. Yasalar önünde sanal dünyada işlenen suçlar her ne kadar artık gerçek dünyadaki gibi suç teşkil etmekteyse de caydırıcı olamamaktadır. İnsanların yaptığı siber saldırılar ve siber zorbalıkların cezasız kalacağı eğilimi toplumlar da gözlenebilmektedir. Siber saldırılar Türk Ceza Kanununa göre suç sayılması insanların gözünde bir nebze de olsa caydırıcılık yaratmak için olumlu bir adımdır.

Bir başka saldırı çeşidi sabit sürücülere herhangi bir zararlı yazılım kaydetme işlemi olmaksızın, yalnızca geçici bellek (RAM) üzerinde işlem yapan "dosyasız" saldırı tipleri de bulunmaktadır.. Bilgisayarınızın belleğinde gizlenerek kullanıcıya farkettirmeden sistem yöneticilerinin şifrelerini topladığı ve hedefinde bulunan kurbanların sistemlerinin uzaktan erişim sağlayarak kontrol edilebildiği siber saldırı tipi de kullanıcılara büyük zararlar verebilmektedir. Dosyasız saldırı ile özellikle finans sektörü öncelikli hedef konumundadır.

En sık karşılaşılan siber saldırı türleri aşağıdaki listede incelenmiştir.

1. Zararlı Yazılımlar (Malware):

Bilgisayar sistemlerini kötü amaçlı kullanmak için sistem bilgilerine erişim sağlamaya yarayan ya da bilgisayar sistemlerine ciddi zararlar veren bilgisayar programlarıdır. Zararlı yazılımlar genel bir kavram olup virüsler, solucanlar, truva atları, rootkitler ve casus yazılımlar bu konseptin içerisinde kendine yer bulabilirler. Zararlı yazılımlar insanlara, süreçlere ve/veya teknolojilere karşı kullanılabilir. Burada ki temel ve en önemli nokta ise zararlı yazılımların amacının sistemlere yetkisiz erişim hakkını elde etmek veya kritik verilerin elde edilmesini sağlanması olduğudur. (İstanbul Üniversitesi Kariyer Geliştirme Uygulama ve Araştırma Merkezi, 2015)

Kişisel bilgisayarlara kullanıcıya fark ettirmeden bulaşarak sahtekarlık, dolandırıcılık ve kimlik hırsızlığı gibi suçların işlenmesine neden olan yazılımlardır. Bunun sonucu olarak, internette alışveriş, bankacılık işlemleri, e-posta alıp gönderme, anında mesajlaşma ve oyun oynama amacıyla gerekli güvenlik programları ve önlemleri olmayan bir bilgisayar kullanıyorsanız kendinizi ve o bilgisayarı kullanan diğer kişileri riske atıyorsunuz diyebiliriz. Bu sebepledir ki kötü amaçlı yazılımlara karşı güvenlik

duvarı, anti virüs ve anti spyware (casus yazılım) programları kullanmanız ve bu programları da güncel tutmanız oldukça önemlidir.

Kötü amaçlı yazılım, zararlı yazılım veya ingilizce kelime olarak malware, mobil cihazların ve bilgisayarların işlevlerini bozmak, kritik bilgileri kopyalamak, kişisel veya kurumsal bilgisayar sistemlerine yetkisiz olarak erişim sağlayabilmek ve istenmeyen reklamları kullanıcıya gösterebilmek için kullanılmakta olan yazılımlar bütününe verilen genel bir kavramdır.

2. Virüsler:

Virüsleri, kullanıcıların bilgisi ve izni dahilinde olmadan gizlice bilgisayarın çalışma prensiplerini değiştirebilen ve kendisini başka dosyaların içerisine kod parçacığı olarak ekleyerek gizlemeye çalışan esasında bir tür bilgisayar programı olarak tarif edebiliriz.

Bilgisayar virüsleri kendini sistemdeki dosyalardan ya da programlar biri olarak değiştiren bilgisayar kodlarıdır. Virüslerin anlaşılmasındaki kritik nokta ise bir kullanıcı tarafından çalıştırılmaları gerektiğidir. Genellikle bir kullanıcıdan gelen e-postanın açılması, ya da USB'nin otomatik çalıştırılması şeklinde meydana gelebilmektedir. (İstanbul Üniversitesi Kariyer Geliştirme Uygulama ve Araştırma Merkezi, 2015)

Virüsler genellikle e-posta mesajlarındaki eklenen dosyalara, anlık sosyal mesajlaşma içeriklerine eklenerek ya da çeşitli donanımsal ve yazılımsal açıklardan yararlanarak bulaşırlar. Bu sebeple özellikle e-posta eklerini, mesajın hangi kişilerden geldiğini bilmiyorsanız veya gelen e-posta size şüpheli göründüyse asla açmamanız önerilir. Virüsler, eğlenceli resimler, tebrik kartları, kutlama mesajları veya görüntü ve ses dosyaları gibi ekler halinde kimliklerini gizleyerek bulaşabilirler. Tanıdık birinden geliyor görüntüsüne bürünerekte mesajlar size iletilebilirler. Anlaşılabileceği üzere u tarz bulaşı yöntemleri sebebi ile işler gerçekten işin içinden çıkılması zor bir duruma gelmektedir ki bu da kullanıcıların daha dikkatli davranması demektir.

Virüsler ayrıca zararlı yazılımlar içeren internet siteleri aracılığıyla veya internette güvenilir olmayan az bilinir sitelerden yapılan karşıdan yüklemeler yoluyla da yayılabilmektedir. Virüsler, zararlı içerik barındıran internet sitelerinin farklı yöntemleri ile istemli ya da istemsiz olarak herhangi bir güvenilir olmayan kaynaktan bilgisayarlara kurulan programlar aracılığıyla, yasalara uygun olmayan şifresi kırılmış yazılımlarda,

karşıdan yüklemek isteyebileceğiniz diğer dosyalarda ve yazılımlarda da gizlenebilmektedirler.

Bilgisayar virüslerinin sisteminize bulaşmaması için bilgisayarınızın sistem güncelleme ve yamalarını güncel tutmanız, antivirüs programlarını otomatik güncellemeye ayarlamanız, dünyada ki en son tehditler hakkındaki haberler konusunda bilgi sahibi olmanız, yönetici haklarıyla bilgisayarınızı çalıştırmak yerine standart kullanıcı ya da misafir kullanıcı olarak kullanmamız, internette gezinti yaparken, sitelerden dosyaları bilgisayarımıza yüklerken ve eklerini açarken bazı temel güvenlik önlemlerine uygun olarak hareket etmek sizi ve sisteminizi güvende tutmaya yarayacaktır.

Eğer ki sisteminize virüs bulaşmıştıysa, virüsün türünü bilmek ve sisteminize bulaşmak için kullandığı yöntemi bilmek, virüsü silmek ve sisteminize daha fazla bulaşmasını engel olmak adına oldukça önem arz etmektedir.

3. Truva Atı:

Bilgisayar kullanıcılarının içeriği hakkında derinlemesine bilgisi olmadan yükledikleri zararlı yazılımlardır. Örneğin bir kullanıcının "Flash Player" yüklediğini düşünürken aslında “Adobe” ya da güvenilir bir kaynak yerine rastgele bir kaynaktan “Flash Player” yüklemesi olarak düşünülebilir. Genel olarak Truva atı olan programlar dosyanın sisteme indirilmesi sonrasında yüklenmesi neticesinde bilgisayar sistemlerine bulaşırlar. Truva atlarının karakteristiği kullanıcı bilgisayarının uzaktan kontrol edilebilmesi ya da izlenmesinin sağlanmasıdır. Truva atı yüklenmiş olduğu bilgisayarların zombi bilgisayarlar olarak da kullanılmasına izin vermektedir. (İstanbul Üniversitesi Kariyer Geliştirme Uygulama ve Araştırma Merkezi, 2015)

Truva atı zararlı kod içeren yazılım olarak adlandırılabilir. Bilgisayar terimi olarak truva atı ülkemizde iyi bilinen Çanakkale civarlarında geçen tarihi truva atı efsanesinden türetilmiştir. Faydalı program ya da bir hediyeymiş gibi kullanıcıya sunulan program gibi görüntü verilen zararlı yazılım çalıştırıldığında siz farkında olmadan bilgilerinize veya diğer kullandığınız programlarınıza zarar verir veya bilgilerinizi izinsiz olarak kopyalayarak istenmeyen üçüncü şahıslarla paylaşmak üzere tasarlanmışlardır.

Truva atı; siber saldırganlara kullanıcıdan habersiz bilgilerinizeve dosyalarınıza ulaşım imkanı sağlar. Fakat bunu doğrudan yapmak yerine truva atının içine saklandığı yazılımı kullanıcıdan çalıştırmasını bekler. Kullanıcı yazılımı çalıştırınca istemsiz olarak truva atı virüsünü sisteme bulaştırmış olmaktadır. Örneğin; "ücretsiz mp3 hit şarkı indir" yazılımını yükleyin gibi bir ifade ile karşılaştığınızda bilinen yasal mp3 müzik indirme programları dışındaki bir yazılımı bilgisayarınıza bulaştırarak sizi kurulan bu tuzağa çekmeleri cazip hale getirilerek mümkün kılınabilir.

Truva atları, bilgisayarları izinsiz olarak, uzaktan erişime açabilirler, elektronik posta gönderebilirler, verilerinizi değiştirebilir ya da bozabilirler, ağ geçitlerinde kendilerini saklayabilirler, ağ içindeki dosya yükleme sistemine bulaşabilirler, güvenlik yazılımınızı istemsiz olarak devre dışı bırakabilirler, hizmet dışı saldırısı ile hizmetin geçici durdurulması veya yavaşlatılması saldırısında bulunabilirler ya da internet erişiminize yavaşlatıp kopmalar yaşamanıza neden olacak saldırıları yapabilirler. Bu bile şirketlere ya da kişilere fazlasıyla maddi ve manevi zarar vermeye yeterli olabilmektedir.

Truva atları, genellikle kullanıcıya meşru yazılım kılığında görünen bir tür kötü amaçlı yazılımdır. Truva atları, kullanıcıların sistemlerine erişmeye çalışan siber hırsızlar ve saldırganlar tarafından kullanılabilir. Genellikle kullanıcıları bir tür sosyal mühendislik kandırmacasıyla kandırarak truva atı yazılımını sistemlerine yükler ve çalıştırarak sistemlerine sızmasına kendi elleriyle izin verirler. Truva atları etkinleştirildikten sonra siber saldırganların sizi takip etmeleri, hassas verilerinizi kopyalamaları ve sisteminize arka kapı erişimi elde etmelerine izin vermiş olursunuz. Bu işlemler arasında şunlar bulunabilir:

- Veriyi silme
- Veriyi engelleme
- Veriyi değiştirme
- Veriyi kopyalama
- Bilgisayarların veya bilgisayar ağlarının sistem performansını düşürme

Truva atlarının diğer bilgisayar virüsleri ve solucanlarından en önemli farkı ise kendi kendilerine çoğalamamaları olarak söylenebilir.

Tanıdığınız birinden ya da kurumdan gelmiş gibi görünen ama şüphenizi çekecek gariplikte ek olarak gözüken bir mail aldığınızda; ek olarak gelen dosyayı tıklayınca direkt indirmek yerine içeriği çok iyi tahlil edip kandırıldığınızı anlayabilirsiniz. Aslında bu gelen mail bir siber suçludan gelmekte ve tıklayıp açtığınız dosya, cihazınıza kötü amaçlı yazılım yüklemeye başlamış oluyor. Yazılımı çalıştırdığınızda kötü amaçlı yazılımı diğer dosyalara bulaştırabilirsiniz ve bilgisayarınıza zarar vermesine neden olabilirsiniz. Truva atları farklı farklı amaçlar doğrultusunda yazılmış çeşitleri bulunmaktadır. Örneğin dosyalarınızı kopyalayarak istenmeyen üçüncü kişilere göndermek, kredi kartı bilgilerinizi kopyalamak, dosyalarınızı silmek, dosyalarınızı bozmak ve kullanılamaz hale getirmek gibi çeşitli zararlar verebilen türleri mevcuttur.

4. Solucanlar:

Virüs gibi kendini bir bilgisayardan başka bilgisayara kopyalamak için tasarlanmış zararlı yazılımlardır. Virüslerden farkı yayılma işlemini ağ üzerinden otomatik olarak yapmasıdır. Otomatik yayılmanın olması nedeni ile zamanla bilgisayar ağının yavaş çalışması, internet sayfalarının geç gelmesine neden olurlar. Solucanların genel yayılma yöntemleri arasında;

- E-posta eki olarak gönderilen dosyalar ile yayılma,
- Web veya FTP kaynağı bağlantısı ile yayılma,
- ICQ veya IRC mesajında gönderilen bağlantılar ile yayılma
- P2P (eşdüzeyler arası) dosya paylaşım ağları üzerinden yayılma sayılabilmektedir.

Bununla birlikte bazı solucanlar, ağ paketleri olarak yayılmaktadır. Bunlar bilgisayar belleğine doğrudan girmekte ve ardından solucan kodu etkinleştirilmektedir. (İstanbul Üniversitesi Kariyer Geliştirme Uygulama ve Araştırma Merkezi, 2015)

Virüslere göre kendi kendini kopyalarken ana bir programa gerek duymaması, kendi kendini çoğaltma işlemini bağımsız yapabilmesi solucanların yayılım hızını oldukça yüksek seviyelere taşımaktadır. Bilgisayar solucanları genel olarak yerel ağ bağlantısını kullanarak veya kullanıcının indirdiği bir dosya sayesinde sisteme sızdıktan sonra yerel ağ veya internet bağlantısı üzerinden kendisinin birden fazla kopyasını yaparak yayılmak suretiyle ağdaki çok iyi korunmayan tüm bilgisayarları ve sunucuları

etkileyerek çoğalmaya devam eder. Ağ solucanının birbirini takip edebilen her bir kopyası da kendi kendine çoğalabildiği için solucanlar internet ve yerel bilgisayar ağları yoluyla oldukça hızlı bir şekilde çoğalma imkanına sahip olurlar.

Daha komplike yapıya sahip olan zararlı yazılımlardan biri olarak değerlendirebiliriz. Solucanlar özellikle e-posta ile gönderilen dosyalardaki ekler, çeşitli internet siteleri ve yerel ağ üzerinde kullanıcıların paylaştığı dosyaları kullanarak bilgisayarlar arasında hızlıca yayılırlar. Solucanlar, bir sistemi yayıldıklarında kullanıcının başka herhangi bir hareketine ihtiyaç duymaksızın, kullanıcının sahip olduğu kayıtlı veri kaynaklarını kullanarak (e-posta kişi ve adres listesi gibi) kendi iletmek istediği kaynak dosyalarını olabildiğince hızlı bir şekilde diğer kullanıcılara da iletmeyi hedeflerler ve bu şekilde kendilerini oldukça kısa sürede çoğaltabilmektedirler. Bunu yaparken solucanlar, kullanıcıların özellikle bant genişliklerini ve sahip olunan ağ kaynaklarını kullandıklarından ağların çalışamaz duruma gelecek kadar kilitlenmesine, e-posta sunucularının normalden fazla olarak aşırı yüklenmesine veya internet kaynaklarına erişim hızının oldukça yavaşlamasına sebep olabilmektedirler.

Virüsler genellikle kullanıcılar veri alışverişi yaptıkça yayılmaktadır, ancak solucanlar internet hızında kendilerini çoğaltabilir. Solucanlar tek bir bilgisayardaki bütün dosyalara bulaşmak yerine olabildiğince çok sayıda bilgisayara ulaşıp bulaştığı bilgisayarda çoğalmayı kendine hedef edinmiştir.

Solucanların ise öncelikli hedefi zarar vermek yerine sadece gezindiğiniz internet sitelerini, girilen kullanıcı adı ve şifrelerinizi, indirdiğiniz programların hangileri ve hangi siteden indirildiklerine dair bilgileri, yani bilgisayarda yaptığınız her şeyi istenmeyenüçüncü kişilere rapor halinde bildirmektir. Solucan ilk iş olarak, bilgisayarda dosya aktarımını sağlayan veya veri iletimi özelliklerinin denetimini ele geçirmeye çalışır. Solucan sisteminize bulaştıktan sonra kendi başına hızlıca çoğalabilir. Solucanların kullanıcılar açısından bakacak olursak en büyük tehlikesi, kendilerini oldukça fazla sayılarda çoğaltabilme kaabiliyetleridir. Örnek verecek olursak, bir solucan e-posta adres defterinizde bulunan tüm kişilerinize bir kopyasını yönlendirebilir ve sonra aynı işlemi onların bilgisayarlarında da yapmaya çalışır. Genellikle solucanlar kullanıcının herhangi bir hareketini beklemeksizin yayılabilir ve kendisinin tam kopyalarını bir ağdan başka ağlara dağıtma işlemini yapabilir. Solucanlar özellikle

bilgisayarın ya da sistemin belleğini veya ağ bant genişliği hızlıca tüketebilir, bunun sonucunda ise bilgisayarın hızının kasmasına ya da tamamen çökmesine neden olabilir.

Solucanlar, kullanıcının herhangi bir etkisi olmadan yayılabilen bir bilgisayar kodudur. Genellikle solucanlar, açıldığında bilgisayara ya da sisteminize virüs bulaştıran e-posta ekleri olarak kendilerini gösterirler. Solucanlar bulaştığı bilgisayarda, adres defterleri veya geçici internet sayfaları gibi e-posta adresleri içeren dosyalarda genel bir tarama yapar. Bilgisayar solucanları, sızdıkları e-posta mesajlarını göndermek için kullanıcının sahip olduğu iletişim adresleri kullanır ve özellikle bu virüslü mesajların tanıdığınız bildiğimiz bir kişiden geliyormuş gibi görünmesini sağlamak adına genellikle sonraki e-posta mesajlarında "Kimden" adreslerini taklit ederek sistemi ve güvenlik yazılımlarını kandırmaya çalışır. Sonraki aşamada solucanlar e-posta mesajlarını, ağların veya işletim sisteminin güvenlik açıklarını kullanarak genellikle yavaşlamaya neden olduran bu sorunun nedeni anlaşılmadan ilgili yerleri ve adresleriotomatik olarak doldurarak yayılma eğilimi gösterirler. Aslında solucanların bilgisayarlara her zaman zarar verdiğini söylemek doğru olmaz, ancak genel olarak bilgisayarın ve ağ performansının oldukça düşmesi ve kararlılık sorunları yaşamasına neden olmaktadır.

Solucanları sisteme çok zarar vermedikleri için diğer virüs çeşitlerine göre hafife almak, kullanıcının bunun bedelini internet hızının ciddi oranda düşmesi, bilgisayar hızınızın aynı oranda etkili bir şekilde etkilenmesi, kişisel bilgi ve şifrelerinizin çalınması şeklinde ciddi sonuçlara katlanması gerektiği sonucunu doğurur.

5. Rootkit:

Bilgisayara bulaşan, çalışan işlemler arasında kendini gizleyen, kötü niyetli kişilere uzaktan bilgisayarınızın tam hakimiyetini sağlayan tespit edilmesi oldukça zor olan bilgisayar programıdır. Virüsler gibi amacı sisteminizi yavaşlatmak ve yayılmak değildir. Bilgisayarınızın kontrolünü ele geçirmek ve bulunduğu sistemde varlığını gizlemektir. Önceleri çok kullanıcılı sistemlerde sıradan kullanıcıların yönetim programlarına ve sistem bilgilerine erişimini gizlemek için geliştirilmiş ve kullanılmış olmasına rağmen, kötü niyetli kullanımına da rastlamak mümkündür. Güvenilir bir kaynaktan geldiğine inanılan bir programın üst düzey yetki ile (root gibi) çalıştırılması zararlı bir rootkitin sisteme kurulmasına sebep olur. Benzer şekilde, çok kullanıcılı bir

sistemde kernel vs açıkları kullanılarak sistemde root yetkisi kazanıp rootkit kurulması en yaygın görülen bulaşma şeklidir. Rootkitin gerçekte hangi dosyaları değiştirdiği, kernele hangi modülü yüklediği, dosya sisteminin neresinde kayıtlı olduğu, hangi ağ servisi üzerinde dinleme yaparak uygun komutla harekete geçeceğini tespit etmek güçtür. Yine de, belli zamanlarda en temel komutların ve muhtemel rootkit bulaşma noktalarının öz değerlerinin saklanarak bunların daha sonra kontrol edilmesi gibi metodlar kullanılabilir. (İstanbul Üniversitesi Kariyer Geliştirme Uygulama ve Araştırma Merkezi, 2015)

Rootkit yani türkçe anlamıyla kök kullanıcı takımı; üzerinde çalışılan süreçleri, açılan dosyaları veya kullanılan işletim sisteminin sistem bilgilerini çalıştığı işletim sisteminden bir yolunu bularak gizlemek kaydıyla varlığını gizlice sürdüren bir program veya programlar grubuna denir. Esas amacı sistemde çoğalmak değil, var olduğu sistemde varlığını gizlemektir. Sistemde varlığını gizlediği sürece kullanıcın farkında olmadan yaptıklarını kayıt altına alarak güvenlik zaafiyeti oluşturmaktadır.

Sorun şu ki Rootkit'in gerçekte hangi dosyalar üzerinde oynama yaptığı, çekirdeğe hangi modülü ya da kod parçacığını yüklediği, bilgisayarın dosya sisteminin tam olarak neresinde kayıtlı olduğu ve hangi ağ servisi üzerinde dinleme yaparak uygun komut satırlarıyla harekete geçeceğini tespit etmek oldukça zordur. Bunlara rağmen rootkit bulaşıp bulaşmadığının tespiti için belli zaman aralıklarında en temel komutların ve olası rootkit bulaşabilecek yerlerin olması gereken normal değerlerinin saklanarak daha sonra bunların kontrol edilip değerlendirilerek rootkit bulaşıp bulaşmadığını analiz edebilmek mümkün olabilir.

Esas amaç rootkitlerde siber saldırganın kullanıcı hesaplarında en yüksek yetkiye sahip olmaya çalışmasıdır. En yüksek yetkiye sahip olan rootkitler kazandığı yetkilerle sistem içerisinde tüm kapıları açabilir ve yönetici yetkisi dahilinde sistem üzerinde her türlü işlemi yapabilir konuma gelebilir.

Aslında rootkitler tek başına tehlikeli sayılmazlar. Buna rağmen virüsler, truva atları ve solucanlar ila beraber siber saldırı açısından inanılmaz bir biçimde tehlikeli olabilirler. Rootkit'ler kullanıcılardan ve de anti-virüs yazılımlarının dijital zararlıların varlığından haberdar olmasına engel oluyor. Genel itibarıyla Windows işletim sisteminin derinliklerine yerleşirler ki bulunmaları daha zor olsun, bu sayede daha uzun

süre farkedilmeden sistem fonksiyonlarını kontrol edebilme imkanına sahip olsunlar. Bu şekilde sisteme bulaşarak Windows gezgini, görev yöneticisi veya virüs tarama işlemlerinin dosya sistemine ilişkin sorgulamalarını yakalamak yoluyla devamında kendilerine ilişkin tüm var olan izleri silerek yok eder ve sorguya sahte bir yanıt vererek sistemi kandırıp gizliliğini sürdürmeye çalışır, bu sayede kötü niyetli çalışmalarını sürdürme fırsatı elde ederler. Sonuç olarak sıklıkla kulanılan araçlar ya da yollarla rootkitlerin izini sürmek sanıldığı gibi kolay değildir. Bazı özel araçlar veya yazılımlar kullanarak rootkitleri bulmak mümkündür. Anti-virüs programları ile taratılan sistemde hiçbir zararlı yazılım bulunmamasına rağmen rootkit tarama araçları veya yazılımları ile aynı sistemi tarattığınızda yüzlerce rootkit bulma ihtimaliniz oldukça yüksektir. Şu unutulmamalıdır ki tamamen güvenli bilgisayar fişi çekili bilgisayar mantığından yola çıkarak sisteminizi mutlaka düzenli olarak sınamanız yararınıza olacaktır.

Rootkit'ler, esas olarak bilgisayarınızda gizli kalabilmeleri için tasarlanmış bir kötü amaçlı yazılım türüdür. En önemli ayrıntı siz onları fark etmeseniz de onlar arka planda aktif olarak çalışırlar. Siber saldırganlara bilgisayarınızı uzaktan kontrol etme hakkını rootkitler kolayca verilebilirler.

Kötü amaçlı yazılım olan rootkitler bilgisayarınızın kontrolünü tamamen sizden alabilir ve siber saldırganların bilgisayarınızı istediği her türlü amaç için kullanması imkanını verebilir. Bilgisayarınız herhangi bir devlet kurumuna karşı yapılan siber saldırıda kullanılabilir, organize suçlara karışabilir, banka ve siber dolandırıcılık suçlarında araç olarak kullanılabilir ve bütün bunlar yaşanırken siz hiç bir şekilde hiç bir şeyin farkında olmayabilirsiniz, fark ettiğinizde ise çok geç kalınmış olabilir. Bu nedenledir ki sisteminizin mutlaka gerekli araç gereçlerle düzenli olarak taratılması gerekmektedir.

Rootkit'ler, bilgisayar korsanlarının şifrelerinizi çalmasına izin veren programlardan kredi kartınızı veya çevrimiçi bankacılık bilgilerinizi çalmasını kolaylaştıran modüllere kadar çeşitli araçlar içerebilir. Rootkit'ler ayrıca bilgisayar korsanlarına güvenlik yazılımını değiştirme veya devre dışı bırakma ve anahtar kelimenize dokunduğunuz tuşları izleme olanağı sunarak suçluların kişisel bilgilerinizi çalmasını kolaylaştırır.

Kök setleri güvenlik yazılımını ele geçirebildiğinden veya bozabildiğinden, bu tür kötü amaçlı yazılımların bilgisayarınızda uzun süre yaşayabileceği ve bu nedenle önemli hasara yol açabileceği tespit edilmiştir. Aslında kendini oldukça iyi gizlemiş bir rootkit kodunu ya da aracını tamamen ortadan kaldırmanın bir tek yolu kalabilir, o da bilgisayarınızın işletim sistemini tamamen silmek veya sıfırdan bütün herşeyi yeniden oluşturmaktır.

Kullanılan işletim sisteminin çekirdeğine rootkitler kendini eklediğinden dolayı bilgisayarımızda yüklü bulunan aktif antivirüs programları rootkitleri genellikle tespit edip bulamaz. Rootkit işletim sisteminin çekirdeğinden veriler gönderip antivirüs yazılımını yanıltma imkanına sahiptir ve çekirdek yazılımına enfekte olduklarından rootkitlerin tespiti imkansız hale gelebilir. Kendini sisteme bulaştıran rootkit eğer yetenekliyse, sistemi temizlemek neredeyse çokta mümkün olmayabilir ve en sonunda bu temizleme işlemi bilgisayarın biçimlendirilmesine neden olabilir.

6. Oltalama / Yemleme (Phishing):

Yasadışı yollarla kullanıcıların herhangi bir sistem için kullandıkları kullanıcı adı, şifre, kimlik bilgileri, kredi kartı ayrıntıları gibi bilgilerin ele geçirilmesidir. Sözcük, İngilizce password (şifre) ve fishing (balık avlamak) sözcüklerinin birleşmesiyle oluşturulmuş phishing ifadesinin Türkçe karşılığıdır. "Yemleyici" diye tanımlanan şifre avcıları, genelde e-posta gibi yollarla kişilere ulaşır ve onların kredi kartı gibi ayrıntılarını sanki resmi bir kurummuş gibi ister. Bu tip mailleri cevaplayan kullanıcıların da hesapları, şifreleri vb. özel bilgileri çalınmaktadır. Örnek olarak; format açısından resmi bir banka konseptinde bir e-posta alınır, ve bu epostada şifre, kredi kartı numarası vb. bilgilerin verilmesi önerilir. Yemleme karşısında tüm bankalar gibi kurumlar hiçbir zaman kullanıcılarından e-posta aracılığı ile özel bilgilerini istemeyeceklerini, böyle bir durumda e-postayı vb. talepleri kendilerine iletmelerini önerirler. (İstanbul Üniversitesi Kariyer Geliştirme Uygulama ve Araştırma Merkezi, 2015)

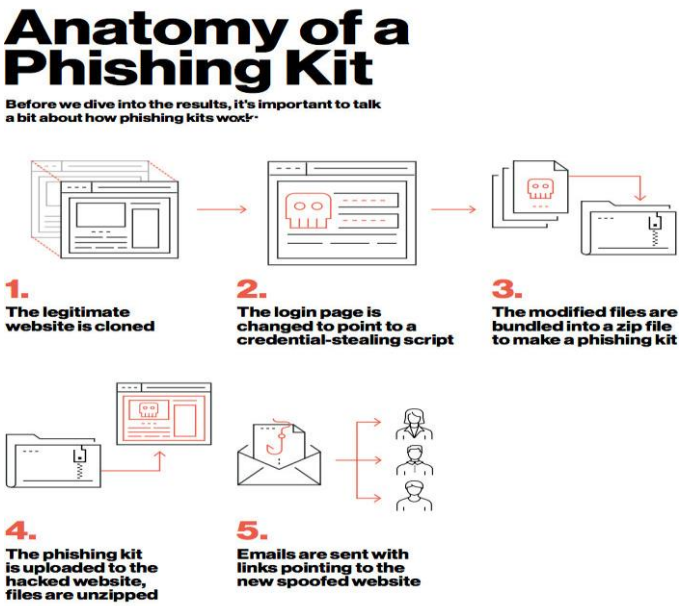
Phishing yani türkçe karşılığı "oltalama", e-postanın içerisine gizlenen silah olarak kullanan bir siber saldırıdır. Amaç, e-posta alıcısını, kullanıcıya gelen e-postayı yine kullanıcının başka bir kullanıcıdan beklediği mesaja, istedikleri veya ihtiyaç duydukları bir şeye (örneğin bankalarından bir talep veya şirketlerindeki bir kişiden

gelen bir not) inandırarak kandırmak amacıyla bir bağlantıyı tıklamak veya bir eki indirmek şeklinde kullanıcın kandırılması amaçlanmıştır.

Phishing kelimesi oltalama, yemleme veya kimlik avı olarakta kullanılmaktadır. Kimlik avını gerçekten ayıran şey, iletinin aldığı biçimdir: saldırganlar, genellikle gerçek veya makul olarak gerçek bir kişi veya kurbanın iş yapabileceği bir şirket olarak güvenilen bir varlık olarak maskelenir. 1990'lara dayanan en eski siber saldırı türlerinden biridir ve kimlik avı mesajları ve teknikleri giderek daha karmaşık hale gelen hala en yaygın ve zararlılardan biridir.

Oltalama saldırısı yapmak için uzman olmaya gerek yoktur. İnternet ortamından bulunup kuracağınız "oltalama kitleri" (Phishing Kit) denilen programlar sayesinde basit teknik bilgi ve beceriniz varsa kolayca kullanılıp siber saldırı yapabilmek oldukça kolay hale gelmiştir. Herhangi bir oltalama kitini yükleyen kullanıcı uzman olmasa bile diğer internet kullanıcıları ve sitelerine artık potansiyel bir tehdit olarak kabul edilebilir. Fakat siber saldırgan olmaya çalışırken indirilen oltalama kitinin içerisine yerleştirilen küçük bir zararlı yazılım kod parçasıyla bir anda avcı olan siber saldırgan, bir başka siber saldırganın avı konumuna düşebilir.

**Şekil 1.** Oltalama Kitinin Anatomisi




**Kaynak:** (FRUHLINGER, 2020)

Şekil 1'de oltalama kitinin anatomisi genel hatlarıyla adım adım belirtilmiştir. Birinci adımda oltalama kiti programı sayesinde herhangi bir yasal internet sitesi kopyalanmış olur. İkinci adımda ise klonlanan internet sitesinde birebir aynı görüntü ile klonlanan giriş sayfası kimlik bilgisi çalma kod parçacığına yönlendirilir. Üçüncü adımda ise giriş sayfasından kullanıcının farkında olmadan sahte siteye yazdığı giriş bilgi ve şifresi, kötü amaçlı kod parçacığı sayesinde oltalama yapabilmek için sıkıştırılarak oltalama yapılacak site ya da kişiye gönderilmek üzere paketlenir. Dördüncü adımda oltalama kiti yazılımı sayesinde hacklenmiş siteden alınan sıkıştırılmış dosyalar açılarak siber saldırganların istediği e-posta veya siteye yüklenir. Son adım olan beşinci adımda ise hacklenen kişinin adres defterinde ki kayıtlı e-posta adreslerine sanki tanıdık ve güvenilir kişiden geliyormuşçasına başlık eklenerek oltalama adı verilen siber saldırı e-postaları yeni kurbanlarına gönderilir. Bu sayede kimlik avı yani oltalama yapılarak siber saldırgan ve saldırganlar tarafından yeni kullanıcı bilgileri kullanıcıya fark ettirilmeden ele geçirilmeye çalışılır.

7. Casus Programlar (Spyware):

Casus programlar bilgisayarınızda casusluk yapmak için yaratılmış programlardır. Casus yazılım, kullanıcılara ait önemli bilgilerin ve kullanıcının yaptığı işlemlerin, kullanıcının bilgisi olmadan toplanmasını ve bu bilgilerin kötü niyetli kişilere gönderilmesini sağlayan yazılım olarak tanımlanır. Bu casus yazılımlar, diğer kötücül yazılımlara göre özellikle İnternet kullanıcıları tarafından sistemlere farkında olmadan bulaştırılmaktadırlar. Casus yazılımlar, virüs ve solucanların aksine sisteme bulaştıktan sonra yayılmaya ihtiyaç duymaz. Amaç, bulaştırılan sistemde gizliliği sağlayarak bilgi toplamaktır. Bu bilgi kimi zaman bir kredi kartı numarası gibi önemli bir bilgi bile olabilir. Bunun dışında, Ticari firmalar İnternet üzerindeki kullanıcı alışkanlıklarını saptamak amacıyla casus yazılımları İnternet üzerinde yayabilmektedirler. (İstanbul Üniversitesi Kariyer Geliştirme Uygulama ve Araştırma Merkezi, 2015)

Casus yazılım, bilgisayarınıza kendini yükleyen ve bilginiz veya izniniz olmadan çevrimiçi davranışınızı gizlice izlemeye başlayan herhangi bir yazılımdır. Casus yazılım, bir kişi veya kuruluş hakkında gizlice bilgi toplayan ve bu verileri diğer taraflara aktaran bir tür kötü amaçlı yazılımdır. Bazı durumlarda, bunlar

reklamverenler veya pazarlama veri firmaları olabilir, bu yüzden casus yazılımlara bazen “adware” denir. Drive-by indirme, yasal bir programa dahil edilmiş bir truva atı veya aldatıcı bir açılır pencere gibi yöntemlerle kullanıcı izni olmadan yüklenir.

Casus yazılımlar, internet bağlantınızı adınız, adresiniz, tarama alışkanlıklarınız, tercihleriniz, ilgi alanlarınız veya indirmeleriniz gibi kişisel bilgileri aktarmak için kullanır. Diğer casus yazılım türleri tarayıcınızı başka bir web sitesine yönlendirmek, cihazınızın arama yapmasına veya metinleri otomatik olarak göndermesine veya çevrimdışı olsanız bile rahatsız edici reklamlar sunmasına neden olur. Kullanıcı adınızı, şifrenizi veya diğer kimlik bilgilerinizi çalan casus yazılımlara “keylogger” denir.

Casus yazılım bulaşma belirtileri istenmeyen davranışları ve sistem performansının düşmesini içerebilir. CPU kapasitesini, disk kullanımını ve ağ trafiğini yiyebilir. Uygulamaların donması, önyükleme başarısızlığı, internete bağlanma zorluğu ve sistem çökmeleri gibi kararlılık sorunları da yaygındır.

Kullanıcı hangi verilerin toplandığını ve kimlerle paylaşıldığını tam olarak anladığı sürece tüm veri toplama programlarına casus yazılım demek doğru değildir. Özellikle pazarlama şirketlerinin çerezleri açısından bakarsak, kullanıcı bilgilerini izleme ve raporlama, yasal yazılım satıcılarının ürünlerini geliştirmelerine veya müşterileri daha iyi desteklemelerine yardımcı olma amacı taşırlar ve bu bakımdan casus yazılımlar ile arasında çok ince bir çigi vardır. Bu nedenle, pazarlama şirketleri genellikle hizmetlerini "casus yazılım" olarak adlandırmaya itiraz ederler. Yasadışı casus yazılımlar ve meşru veri toplama arasındaki çizgi genellikle bireylerin cihazlarında internet davranışı hakkında bilgi depolamanın bilinen bir yöntemi olan çerezlerde çizilir. Bazı kullanıcılar çerezlere izin verir, bazıları ise çerezlerden tam anlamıyla hoşnutsuzluk duygusu taşıyarak olaya bakarlar.

Casus yazılım bir tür kötü amaçlı yazılımdır ve kullanıcının izni olmadan bir bilgisayar veya ağ hakkında bilgi toplar ve paylaşır. Orijinal yazılım paketlerinin gizli bir bileşeni olarak veya aldatıcı reklamlar, web siteleri, e-posta, anlık mesajlar ve doğrudan dosya paylaşım bağlantıları gibi geleneksel kötü amaçlı yazılım vektörleri aracılığıyla yüklenebilir. Diğer kötü amaçlı yazılım türlerinden farklı olarak, casus yazılımlar sadece suç örgütleri tarafından değil, aynı zamanda vicdansız reklamverenler ve rızası olmadan kullanıcılardan piyasa verilerini toplamak için casus yazılım kullanan

şirketler tarafından da yoğun bir şekilde kullanılmaktadır. Kaynağından bağımsız olarak, casus yazılımlar kullanıcıdan gizlenir ve algılanması genellikle zordur, ancak sistem performansının bozulması ve istenmeyen davranışların sıklığı (pop-up'lar, yönlendirilmiş tarayıcı ana sayfası, arama sonuçları vb.) gibi belirtilere yol açabilir.

Casus yazılımlar aynı zamanda ağ oluşturma özellikleriyle de dikkate değerdir. Casus yazılım bu bilgileri saldırgana geri gönderemezse, bilgileri bulmak için virüslü bir sistem kullanmak çok az değer taşır. Sonuç olarak, casus yazılım, bir saldırganla şüphe yaratmayacak veya ağ güvenlik ekiplerinden dikkat çekmeyecek şekilde iletişim kurmak için çeşitli teknikler kullanır.

Reklamcılık için bir araç olarak, casus yazılımlar, ilgili reklam verenlere veya diğer ilgili taraflara kullanıcı bilgilerini toplamak ve satmak için kullanılır. Casus yazılımlar, internette gezinme alışkanlıkları ve indirme etkinliği de dahil olmak üzere neredeyse her türlü veriyi toplayabilir. Belki de casus yazılımlarla ilgili en büyük endişe, varlığı tespit edilip edilmediğine bakılmaksızın, kullanıcının hangi bilgilerin yakalandığı, gönderildiği veya kullanıldığına dair herhangi bir fikre veya ne bulmak için herhangi bir mekanizmaya veya teknolojiye sahip olmasıdır.

Casus yazılımlar, kullanıcının adı, adresi, parolaları, banka ve kredi bilgileri ve sosyal güvenlik bilgileri gibi kişisel ayrıntıları elde etmek için tuş kaydedicileri kullanabilir. Dosyaları sistemin sabit diskine tarayabilir, diğer uygulamaları arayabilir, ek casus yazılım yükleyebilir, çerezleri okuyabilir ve sistemin internet ayarlarını ve dinamik olarak bağlı kütüphaneleri (DLL) değiştirebilir. Bu, güvenlik ayarlarının düşmesine (kötü amaçlı yazılımlara daha fazla davet etmek için) ve internet ile bilgisayardaki arızaların, ister çevrimiçi ister çevrimdışı olsun, sistemin internet ayarlarında derinden kaynaklı bağlantı hatalarına kadar değişen arızalara neden olabilir. Bu değişikliklerin bir çoğunu, etkilenen cihazı yeniden görüntülemeden geri almak veya kurtarmak oldukça zordur.

Casus yazılımların virüs bulaşmış bilgisayarlara verdiği tehditlere ek olarak, çoğu zaman işlemci gücünü, RAM'i, diskleri ve ağ trafiğini de barındıran önemli bir sistem kaynağı tüketicisi olabilir. Sonuçta ortaya çıkan performans düşüşü çökmelere veya genel sistem kararsızlığına neden olabilir. Bazı casus yazılımlar, rakip casus

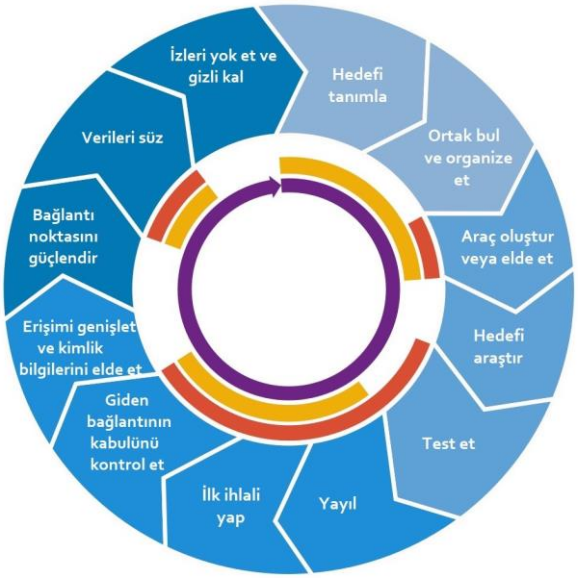
yazılım programlarını devre dışı bırakır veya ortadan kaldırır ve kullanıcının programı kaldırma girişimlerini algılayabilir ve engelleyebilir.

Casus yazılımlar, uç nokta ve ağ güvenliği denetimlerinin bir kombinasyonu ile önlenebilir. Casus yazılım önleme özellikleri genellikle uç noktada koruma sağlayan modern antivirüs yazılımı ürünlerine entegre edilir. Casus yazılımların ağ üzerinden iletişim kurması gerektiği göz önüne alındığında, casus yazılımlar da casus yazılım iletişiminin algılanabileceği ve engellenebileceği ağ güvenliği katmanında giderek daha fazla kontrol edilmektedir. Buna ek olarak, sürücü indirme korumaları, tarayıcının pop-up engelleyicisi kullanılarak ve kullanıcının izni olmadan dosya indirilmesini önleyen yeni nesil ağ denetimleri kullanılarak bitiş noktasında uygulanabilir. Son olarak, hangi yazılım bileşenlerinin, eklentilerin ve hizmetlerin bir cihazda ve ağ üzerinde çalışmasına izin verildiğini izlemek ve doğrulamak kullanıcıların siber saldırıya uğramaması açısından önemlidir.

8. Sosyal Mühendislik:

Temel olarak bilgisayar ya da bilgisayar ağlarındaki açıklıklardan faydalanarak bilgisayar sistemlerine zarar veren yaklaşımların aksine “sosyal mühendislik” yöntemi insanların iletişim, düşünce tarzı, güven ya da kısaca insani zaaflarından faydalanarak siber güvenlik süreçlerinin etkisiz hale getirilmesi ya da atlatılması şeklinde tanımlanabilir. Sosyal mühendislik yöntemleri; çeşitli yalanlar yolu ile sahte senaryolar üretmek, hedef kişiye kendini güvenilir bir kaynak olarak tanıtmak ya da basit ödüllendirme yöntemleri ile bilgi sızdırmak şeklinde özetlenebilir. (İstanbul Üniversitesi Kariyer Geliştirme Uygulama ve Araştırma Merkezi, 2015)

**Şekil 2.** Sosyal Mühendislik Saldırılarının Yaşam Döngüsü




**Kaynak** (BAŞAKÇI, 2019)

Sosyal mühendislik, insanların zaaflarını kullanarak kandırma yoluyla gerçekleştirilen çok çeşitli kötü amaçlı işlemler için kullanılan bir kavramdır. Kullanıcıları güvenlik hataları yapmak veya hassas bilgileri vermek için kandırmak için psikolojik manipülasyon kullanır.

Şekil 2'de sosyal mühendislik saldırıları yapılırken kullanılan yöntelerinr yaşam döngüsü genel hatlarıyla verilmiştir. Bu adımlar bir veya daha fazla adımda da gerçekleşeir. Bir fail ilk olarak, saldırıyı sürdürmek için gereken potansiyel sisteme sızma noktaları ve iyi yapılandırılmamış zayıf güvenlik protokolleri gibi gerekli arka plan bilgilerini toplamak için hedeflenen kurbanı araştırır. Ardından, saldırgan, mağdurun güvenini kazanmak için hareket eder ve hassas bilgileri ortaya çıkarmak veya kritik kaynaklara erişim vermek gibi güvenlik uygulamalarını bozan sonraki eylemler için uyarıcılar sağlar.

Sosyal mühendisliği özellikle tehlikeli yapan şey, yazılım ve işletim sistemlerindeki güvenlik açıklarından ziyade insan hatasına dayanmasıdır. Meşru kullanıcılar tarafından yapılan hatalar, daha az öngörülebilirdir, bu da onları kötü amaçlı yazılım tabanlı bir saldırıya göre tanımlamayı ve engellemeyi zorlaştırır.

Sosyal mühendislik insanları manipüle etme sanatıdır, bu yüzden gizli bilgilerden vazgeçerler. Bu suçluların aradıkları bilgi türleri değişebilir, ancak bireyler hedeflendiğinde suçlular genellikle parolalarınızı veya banka bilgilerinizi vermeniz için sizi kandırmaya çalışır veya kötü amaçlı yazılımları gizlice yüklemek için bilgisayarınıza erişir; şifreler ve banka bilgilerinin yanı sıra bilgisayarınız üzerinde kontrol sahibi olmalarını sağlar.

Suçlular sosyal mühendislik taktikleri kullanır, çünkü doğal eğilimlerinizi güvendiğinizden yararlanmak genellikle yazılımınızı hacklemenin yollarını keşfetmekten daha kolaydır. Örneğin, birisinin size şifresini vermesini kandırmak çok daha kolaydır (şifre gerçekten zayıf olmadıkça).

Siber saldırgan, bir kişinin e-posta şifresini hacklemeyi veya sosyal olarak mühendisliği yapmayı başarırsa, o kişinin kişi listesine erişebilir ve çoğu kişi her yerde bir şifre kullandığından, muhtemelen o kişinin sosyal ağ kişilerine de erişebilir.

Siber saldırgan, bu e-posta hesabını kontrol altına aldıktan sonra, tüm kişilerin kişilerine e-posta gönderir veya arkadaşlarının tüm sosyal sayfalarında ve muhtemelen arkadaşlarının arkadaşlarının sayfalarında mesaj bırakır. Böylelikle sosyal mühendislik sayesinde kullanıcı zaaflarını kullanarak sisteme sızabilir ve kişisel bilgilere ya da kurumsal bilgilere erişim sağlayabilirler.

**Hacker ve Cracker Nedir?**

Ülkemizde aslında birbirinden farklı olan bu iki terim için bir kavram karmaşası olduğu gözlenmektedir. Ülkemizde hackerlar çoğunlukla cracker kimlikleri ile ön plana çıktıkları için sistemlere izinsiz girerek zarar veren amacı güden kötü kişiler olarak kendilerinin tanınmalarına neden olmuşlardır. Halbuki bu iki teriminde ne anlama geldiğini detaylı olarak incelediğimizde aslına bakacak olursak ikisinin de aslında birbirinden çok farklı kavramlar olduğunu göreceğiz.

Bütün işletim sistemlerinin yapısı ve ayrıntılarıyla ilgilenen kişilere hacker denilmektedir. Hackerlar genellikle oldukça iyi programlama bilgisine sahip insanlardır. İşletim sistemleri hakkında ve programlama dilleri ile ilgili oldukça üst düzeyde bilgi ve beceriye sahiptirler. Sızdıkları işletim sistemlerinde buldukları açıkları ve bunlara neden olan sebepleri tüm ayrıntılarıyla bilirler ve tüm bunlardan önemlisi hackerlar her zaman

daha fazla birşeyler öğrenmek için durmaksızın kendilerini geliştirirler ve de öğrendiklerini diğer hackerlarla ve gruplarıyla paylaşırlar. Asla hiç bir zaman kasıtlı birilerine zarar verme kastıyla hareker etmezler.

Hackerlarla karıştırılan crackerlar ise kötü niyetli olan kişilerdir ve sistemlere sızdıklarında veri hırsızlığı yaparlar ve girdikleri sistemede zarar verme eğilimi gösterirler. Yasal olmadığını bildikleri halde çoğu zaman bu onlar için caydırıcılık teşkil etmez hatta cazip hale bile getirebilir. Crackerlardan hedeflerine sızmayı başarabilenleri önemli verileri izinsiz silebilir veya sistemin işleyişini kitleyebilirler, aslında gittikleri her yere sorunları da beraberinde götürdüklerini söylemek daha doğru olacaktır. Yaptıkları bu kötü niyetleri eylemler yüzünden crackerları tanımak oldukça kolaydır. Yaptıkları iş ve işlemlerde kanunsuz yolları takip ederler.

Türk Dil Kurumu(2005) Internet sitesinin Yabancı Kelimelere Karşılıklar bölümünde, "Hacker" kelimesinin karşılığı olarak: "Bilgisayar haberleşme teknolojileri konusunda bilgi sahibi olan, bilgisayar programlama alanında standardın üzerinde beceriye sahip bulunan ve böylece ileri düzeyde yazılımlar geliştiren kişi anlamında kullanılan kelime" denmekte ve bu kelime için de "kırıcı" sözcüğü önerilmektedir. Yine, Türk Dil Kurumu(2005)"nun bu kez Bilgisayar Terimleri Karşılıkları bölümünde ise, Hacker: "Çökertici, korsan" kelimeleriyle karşılanmaktadır. Cracker için: "Bir başkasının bilgisayarına girmek, ele geçirmek için teknik ve kişisel becerilerini kullanan kişi" denmektedir. T.D.K."nın Yabancı Kelimelere Karşılıklar bölümünde ise Cracker kelimesi için: Zevk için bilgisayar sistemlerine zarar veren kişi anlamında "çökertici" sözü teklif edilmiştir. (ERİŞ, 2009)

**Siber Saldırılara Karşı Güvenlik Tedbirleri**

Siber güvenlik, "siber ortamda, kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünüdür" şeklinde tarif edilebilir. (Yılmaz & Sağıroğlu, 2013)

Çağımızda artık işletmelere yönelik siber saldırılar kaçınılmaz bir hal almış gibi görünüyor. Ancak bilişim uzmanları, şirketlerini ve işletmelerini siber saldırılara karşı

korumak için aşağıdaki belirtilen adımları uygulayarak, sistemlerine yapılacak olan bu saldırıların çoğunun büyük ölçüde önleyebilmek mümkün hale gelebilir.

- Şirketlere siber saldırıları önlemek için ilk ve en önemli çözüm, parola korumalı ve iki yönlü kimlik doğrulama ile desteklenen güvenli ve sofistike bir donanıma sahip olmaktır . Ayrıca, fiziksel depolama disklerinizi korumanın etkinliğini göz ardı etmemekte iyi olacaktır. Çünkü ihmal edilirse, herkese firmanızın hassas verilerini kopyalama fırsatı verir.
- Şirketinizin donanımını koruyun. Veri ihlallerinin çoğunun çalınan ekipman bilgisayar korsanlarının ellerine ulaştığında gerçekleştiği belirtiliyor. Örneğin, Ar-Ge'de çalışan çalışanlarınızdan biri dizüstü bilgisayarını kaybederse, hassas veriler rakiplerin veya kötü niyetleri olan kişilerin eline ulaşırsa, çalıştığı şirket ciddi sıkıntılara düşebilir. Bu nedenle, herhangi bir istenmeyen olay meydana gelmeden önce bazı fiziksel güvenlik stratejilerini özetlemek daha iyidir. Birden çok güvenlik katmanı tarafından korunan verileri bulutta depolamak ve iş ortamınız için çalışan çalışanlar arasında sorumlu BYOD güvenlik politikaları uygulamak gibi.
- Şirketinizin verilerini şifreleyin. Verilerin yanlış ellere geçmesi durumunda verilerin şifrelenmesi şirketinize üstünlük sağlar. Ve bu, bir hacker onu ele geçirse bile işe yaramaz halde olduğu için hiçbir anlam ifade etmeyecektir.
- Verilerinizi mutlaka güvenilir ortamlarda yedekleyin. Bazen ne kadar zor denerseniz deneyin, bilgisayar korsanları ağınıza girer ve verilerinizi fidye yazılımı ile şifrelemeye çalışırlar. Ancak teşebbüsünüzün en güncel yedek kopyası varsa, sizin veya şirketinizin bilgisayar korsanlarının taleplerini karşılamanıza gerek kalmayacaktır. Ancak unutmayın, yedekleme etkili bir şekilde yapılmalı ve bir felaket meydana gelir gelmez bu da hızlıca geri alınabilir olmalıdır.
- Bireysel ve ticari siber güvenlik sigortası yaptırmak son derece akıllıca bir adım olacaktır. Siber suçlular bugünlerde çok sofistike olduklarından, en gelişmiş siber savunma sistemlerine girmenin yollarını arıyorlar. Bu nedenle, güvenlik konusunda en bilinçli işletmeler bile siber saldırılara karşı savunmasız kalır. Yaptırdığınız sigorta sayesinde bir saldırı meydana geldiği durumlarda sigortaların çoğu sadece veri hırsızlığından kaynaklanan finansal kaybı kapsamakla kalmaz, aynı zamanda veri kurtarma uzmanlarına ödeme yapmayı ve yeni donanım satın almayı da içerir.

- Çalışanları siber ortamdaki en son gelişmeler hakkında eğitin, böylece siber riskleri kolaylıkla azaltmaya yardımcı olabilirler. Bu, çalışma bilgilerine erişmek için güvenli olmayan ağları kullanma ve güvenli olmayan internet sitelerinden kaçınma ve hassas verileri sosyal medyada paylaşma ile ilgili riskler hakkında onları eğitmeyi içerir. Çalışanlarınızı şifre paylaşımından kısıtlamak da siber saldırılardan korunmanıza yardımcı olacaktır.
- Kötü amaçlı yazılımdan koruma çözümlerinin kullanılması ve kurumsal ağların verimli güvenlik duvarlarıyla korunması, kuruluşunuzun BT'sini saldırılara karşı korumaya yardımcı olacaktır.

# BÖLÜM 3. GERÇEK VE SANAL SİBER SALDIRI SENARYOLARI VE OLASI ETKİLERİ

Artık siber saldırılar bilişim teknolojilerini (IT) ilgilendiren bir konu olmaktan çıkıp çerçevesi oldukça genişlemiştir. Örneğin ülkelerin sağlık, enerji, eğitim, askeri alanları, bankacılık sistemi gibi krittik bir çok alan hedef haline gelmiştir. Düzenlenen bu siber saldırılar sayesinde bakalara sızabilmekte, SCADA tabanlı enerji sistemlerini devre dışı bırakabilmekte, iletişim kanallarına sızarak ülkeler arası casusluk yapılabilmekte ya da kişisel bilgiler ele geçirilebilmekte, kişisel e-posta adres defterleri ele geçirilerek istenilen amaç doğrultusunda kullanılabilmekte, evdeki akıllı televizyonların kamerasını ele geçirerek izinsiz kayıt alınabilmekte, ev ağına sızarak kombi veya klima sistemi izinsiz çalıştırılabilmekte, kişisel bilgi ve belgeler yasa dışı bu yolla çoğaltılabilmektedir. Bu ve bunun gibi bir sürü işlemi yapabilen siber saldırganlar artık teknolojik hayatımızın ayrılmaz bir parçası haline gelmiştir.

Aşağıda farklı farklı sanal veya gerçek saldırı senaryoları uygulanmış olup, oluşabilecek senaryolardan doğan sonuçlar detaylarıyla incelenmiştir.

- Senaryo 1: Fiziksel Uygulama Senaryosu

Fiziksel anlamda saldırı yapılacak sisteme müdahale edebilecek kadar yakın olunduğu durumlarda sistemin şifresini ele geçirmek son derece basit bir hal almıştır. Siber saldırganın şifresini öğrenmek istediği bilgisayarın başına oturduğunda o bilgisayarın yönetici şifresini öğrenmesi ya da kendine yönetici olarak bir kullanıcı hesabı açması artık çok zor değil. Şekil 3'te "utilman.exe" programı sayesinde siber saldırgan kendisine sistemde yeni bir kullanıcı adı açıp buna yönetici yetkisi verebilir.

**Şekil 3.** Fiziksel Uygulama Senaryosu




**Kaynak :** (YİĞİT & AKYILDIZ, 2014)

Bu işlemi yapmak için Windows işletim sisteminin kullanıcı parolası sorduğu giriş ekranında siber saldırgan Şekil 3'te sol alt köşede gösterilen simgenin içerisine "cmd.exe" dosyası kopyalanır. Bu sayede aynı simge komut sistemi olarak "cmd.exe" ile tekrar açılıp, "utilman.exe" programıyla terminal olarak çalıştırılır. "utilman.exe" programı sayesinde terminal olarak yönetilen bilgisayarda yönetici kullanıcı adıyla yeni bir hesap oluşturulabilir.

Daha sonra tanımlanan kullanıcı ile sisteme admin yetkisi ile giriş yapılmıştır. Bilgisayar Backtrack Linux işletim sistemi ile açılarak, cmd.exe ve utilman.exe dosyası üzerine kopyalanmıştır. (Yiğit & Akyıldız, 2014)

Fiziksel müdahale sayesinde siber saldırgan sisteme sızarak çeşitli programlar ve komut sisteminde yaptıkları sayesinde kendisine ait yönetici yetkili bir kullanıcı hesabı oluşturması çok kısa bir zamanda mümkün olmuştur. Bu aşamadan sonra siber saldırganın yönetici yetkisini arkasına alarak yapabileceklerinin sınırı yoktur. Bir kullanıcının yönetici hakkıyla bilgisayarda yapabilecekleri bütün işlemleri siber saldırganda yönetici olduğu için yapabilir.

Yapılan bu siber saldırı sonucunda ise yönetici kullanıcıhaklarını kullanan siber saldırgan bilgisayardaki tüm verileri silebilir, değiştirebilir, yine bilgisayarda bulunan kişisel veya kurumsal kayıtlı bulunan tüm şifrelere erişip kullanabilir, bankacılık şifresini hatırlatma olarak bir yere yazdıysanız sizin kredi kartlarınızla alışveriş yapabilir, banka hesabınızdan havale ve EFT gibi işlemle sizin banka hesabınızı boşaltabilme imkanına kavuşabilir. Sizin adınıza bağlı olduğu ağ üzerinden başka

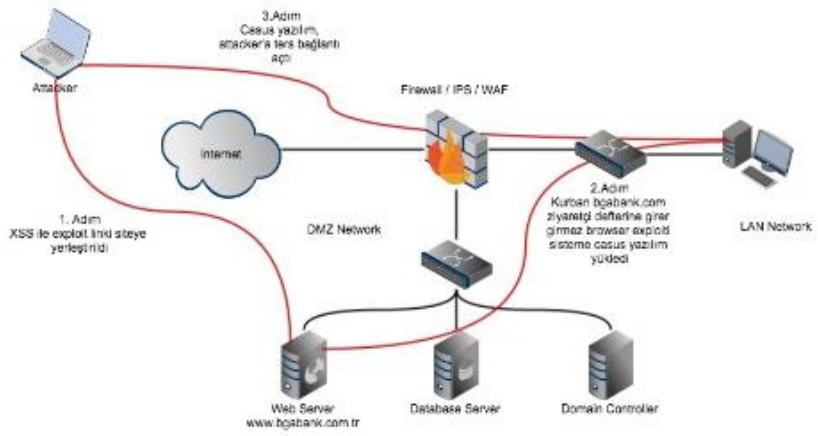
arkadaşlarınız ya da şirket çalışanlarıyla onlarında kişisel bilgilerine sosyal mühendislik kullanarak sanki sizle konuşuyormuş hissi vererek dolandırıcılık yapabilir.

- Senaryo 2: Bankanın Ziyaretçi Defterindeki XSS Açığı Sayesinde Zararlı Yazılım Bulaştırma Senaryosu

Gerçek bir bankanın ziyaretçi defterindeki açığı kullanarak, ziyaretçi defterine yazı yazan kullanıcıların her birine zararlı yazılım bulaştırmak kaydıyla yapılan siber saldırı ve sonuçlarını beraber değerlendireceğiz.

Siber saldırgan bankanın www.bgbank.com domain adresine girerek, kullanıcıların doldurduğu ziyaretçi defterinde "stored XSS" (saklanan XSS) dosya bilgilerinde açık kapı zaafiyeti bulmuştur.

**Şekil 4.** Gerçek Banka Siber Saldırı Senaryosu




**Kaynak** : (UÇAR, 2015)

XSS 2014 yılında da en çok keşfedilen ve risk seviyesi yüksek web tabanlı güvenlik zaafiyetidir. (Uçar, 2015)

Ziyaretçi defterinde bulunan "stored XSS" zaafiyetini kullanan siber saldırgan kurbanları olan banka müşterilerine zararlı yazılımları bu açığı kullanarak bulaştırmaya çalışır.

**Şekil 5.** Ziyaretçi Defteri Açıldığında Otomatik Yüklenen Zararlı Yazılım




**Kaynak :** (UÇAR, 2015)

Banka müşterisi olan siber saldırı mağduru fark etmeden sistemine ziyaretçi defteri açılır açılmaz otomatik olarak Şekil 6'daki "meterpreter" casus yazılımı yüklenmiş olur.

**ŞEKİL 6.** SİSTEME ZARARLI YAZILIM SIZMASI

```
msf exploit(ms14_064_ole_code_execution) > sessions

Active sessions
===============

  Id  Type                   Information                Connection
  --  ----                   -----------                ----------
  3   meterpreter x86/win32  BGAPENTEST\randan @ BGA-PC  104.236.1.47:4444 -> 85.105.101.253:48396 (6.6.6.64)
```

KAYNAK : (UÇAR, 2015)

Bu zararlı yazılımın yüklenmesi ile MS14-068 gibi hak yükseltme zaafiyetlerini kullanarak sisteme sızan zararlı yazılım istenmeyen kullanıcının domainde daha yüksek yetkilere veya yönetici yetkilerine sahip olmak kaydı ile sızılan sistemde daha etkin rol alıp yetki genişliğiyle istediği hamleleri yapmayı daha kolay hale getirmeye çalışır. Domain haklarını elde ettiğinde ise windows işletim sistemine sahip ortamdaki tüm sistemlere en yetkili kullanıcı olarak erişim kurar. Şekil 7'de siber saldırganın sistemdeki kullanıcı adını öğrenip daha geniş yönetici yetkilerine sahip olma aşaması verilmiştir.

**Şekil 7.** Siber Saldırganın Yönetici Kullanıcı Hakkı Elde Etme Adımları




**Kaynak :** (UÇAR, 2015)

TGT saldırısı ile oluşturduğu yeni bilet (ticket) kısıtlı kullanıcı haklarına sahip kullanıcıyı Domain Yöneticisi yetkilerine sahip bir hale getirmiştir. Bu sayede sınırsız kullanıcı yetkileriyle bulaştığı banka müşterisinin kayıtlı banka bilgilerine erişim, bilgisayarındaki dosyalara tam erişim hakkı, kayıtlı şifrelere erişim hakkı, internet site kullanım trafik bilerine erişim sağlama, keylogger tarzı programlarla kullanıcının her yazdığını takip edebilmek hakkına sahip olan siber saldırganın kullanıcıya vereceğim maddi ve manevi kayıplar sadece siber saldırganın insafına bırakılmış olur. Malesef ki kötü niyetli saldırganında sisteme ve kurbana insaflı davranarak az zarar vermesini

beklemek pekte akıllıca bir adım olmaz. Bu yüzden mutlaka sistemin güvenlik önlemleri aktif ve güncel tutulmalıdır. Gerekirse kurumsal firmalar için özellikle profesyonel çözümler ve güvenlik yardımları almaları elzem önem taşımaktadır.

Bu saldırı senaryo amacı taşıdığından sistem yöneticisindeki olay kayıtlarına bakıldığında Şekil 8'de görüldüğü gibi arkamızda bazı olay kayıtları (log) bıraktığımızı görebilirsiniz.

**Şekil 8.** Wındows Güvenlik Kayıtları - Olay Özellikleri



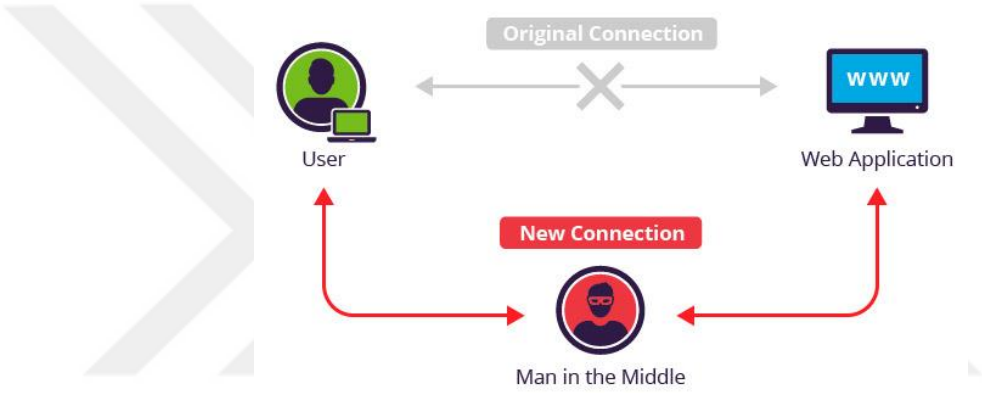

**Kaynak :** (UÇAR, 2015)

Bu yöntemle yapılan saldırılardan korunup maddi ve manevi anlamda zarar görmek istemiyorsak eğer, tüm logların anlamlandırılması ve birbiriyle ilişkilendirilmesi tehlikenin önceden farkedilebilmesi adına iyi olacaktır. Bununla beraber sistemde oluşan yüksek yetki taleplerini incelemek yerinde olacaktır. Ayrıca Siber Olaylara Müdahale Ekibi (SOME) kurmak kaydıyla siber olaylara anında müdahale edip anlamlandırıcak ve çözüme kavuşturacak güvenlik uzmanları olası maddi ve manevi kayıpların önüne geçmenizde oldukça fayda sağlayacaktır.

- Senaryo 3: Yerel Ağda (LAN) Yapılan Ortadaki Adam Saldırı (MITM) Senaryosu

Birçok kuruluşta ya da kamu kurumunda dışarıdan yapılabilecek siber saldırılara karşı oldukça iyi güvenlik önlemleri şirketler tarafından zaten alınmaktadır. Alınan yüksek güvenlik önlemleri sayesinde dışarıdan sızmaların ciddi anlamda önüne geçilmektedir. Fakat şirketlerce göz ardı edilen bir durum vardır. Bu durum ise kendi kullandıkları yerel ağda yani güvenli sandıkları iç ağlarında aslında tehlike göz ardı edilemeyecek kadar büyüktür. Bunun sebebi ise kullanıcıların ya da şirketin güvenlik uzmanlarının kendi yerel ağında kendilerini çok güvende hissetmeleri ve rahat davranmaları gösterilebilir.

**Şekil 9.** Ortadaki Adam Saldırı Mantığı




**Kaynak :** (UFER MEDİA, 2019)

Şekil 9'da belirtildiği gibi yerel ağınızda düzenlenen ortadaki adam saldırısı, siz kendi ağınızda dolaşıyor sanırken bulaşan virüs sayesinde sizi başka bir köprü üzerinden internette ve yerel ağınızda gezinmeniz için yönlendirir. Siz hiç bir şey anlamadan virüs internete çıkmak ya da yerel ağda iletişim kurmak istediğinizde sürekli olarak ağ geçidini kendiymiş gibi göstermeye çalışır. Bir süre içerisinde sistemi kandıran bu virüs sizin girdiğiniz güvenli ağı devre dışı bırakarak kendi ağ geçidi üzerine bütün ağ trafiğini yönlendirir. Ağ trafiğinin tamamını kendi ağ geçiti üzerinden kontrol eden virüs, bu sayede yaptığınız her işlemi filtreleyebilir.

Bu işlemin sonucunda kullanıcıların bütün girdiği internet siteleri, kurum içi veya dışı yazışmaları, girdiği bankacılık ve diğer şifre bilgileri gibi bilgisayar ekranında her attığı adımın ve yazdığı yazıların kaydı tutulur ve siber saldırgan tarafından kullanıcıya hissettirilmeden filtrelenir. Bu sayede kurum içi veya dışı yazışmalardan

elde edilen bilgilerle sanayi ve teknoloji casusluğu, bankacılık dolandırıcılığı, gizli belge ve bilgilerin el değiştirmesi, oluşabilecek kurumsal maddi kayıplar ve bunların yanında görünmeyen kısımda yer alan şirketin itibar kaybı gibi manevi kayba uğraması içten bile değildir.

**Şekil 10.** Lan'da Ortadaki Adam Saldırı Senaryosu




**Kaynak :** (YİĞİT & AKYILDIZ, 2014)

Şekil 10'da kurum içerisinde bulunan yerel ağda gerçekleşen bir ortadaki adam saldırısı gösterilmiştir.

Ortadaki adam saldırısına uğrayan kullanıcının trafiği HTTP ile akmakta olup şifreleri Şekil 10'daki gibi alınmıştır. (Yiğit & Akyıldız, 2014)

- Senaryo 4: ABD Enerji Sistemlerine Yapılan Siber Saldırı Senaryosu

Amerika Birleşik Devletlerinde (ABD) enerji sistemlerine yapılacak olan siber saldırı ile oluşacak olası sonuçlar ülkenin ciddi anlamda etkilenmesine neden olacak derin izler açabilecek büyüklüktedir.

Cambridge Üniversitesi Risk Analizi Merkezi ile Lloyd'un ortak çalışmasına göre elektrik şebekeleri, ülkede yaşanan siber saldırıların hedefleri arasında yüzde 32 ile ilk sırada yer alıyor. Üretim tesisleri ise ikinci sırada bulunuyor. Rapordaki baz senaryo, siber saldırı sonrasında 15 eyalet ve Washington'da yaşanabilecek uzun süreli bir elektrik kesintisinin olası sonuçlarını içeriyor. Yaklaşık 93 milyonluk bir nüfusun etkilenebileceği olası kesinti senaryosu için gerçek verilerle bazı öngörüler bir arada

kullanılmış. Bu senaryoya göre, elektrik şebekesine yönelik olası bir siber saldırı ulaşım sistemlerinin çökmesine, ticaret ve üretimin durmasına, su kesintilerinin yaşanmasına ve hatta ciddi ölümlere yol açabilecek. (enerjigunlugu.net, 2015)

Senaryoya göre, kötü amaçlı bir yazılım ABD'nin Kuzey eyaletlerindeki elektrik santrallerinin kontrol odalarını ele geçiriyor. Yaklaşık 1.5-2 yıl önce başlayan saldırı hazırlıkları sonrası, senaryonun kapsama alanındaki 50'ye yakın üretim tesisinin yaklaşık yüzde 10'unun siber güvenlik duvarları aşılıyor. Hedeflenen bir tarihte, zaman zaman yangınlara da yol açabilecek ölçüde aşırı yüklenmeler yaşanıyor ve bunun sonucunda elektrik üretim tesisleri devreden çıkıyor. Tesislerin devreden çıkması, ABD'nin Kuzey eyaletlerindeki elektrik şebekesini dengesizliğe düşürüyor. Bu da ülkede kalıcı elektrik kesintilerinin ortaya çıkmasına yol açıyor. Kesintilerin bir bölümü ilk 24 saat içinde giderilebiliyor ancak bazı kesimlerde bu kesintiler haftalarca devam ediyor. (enerjigunlugu.net, 2015)

Baz senaryoda 50 üretim tesisi devre dışı kalırken, şebekenin yüzde 90'lık kısmı ancak iki haftalık bir sürenin sonunda yeniden ayağa kaldırılabiliyor. Senaryoya göre, bu süreçte şehirler yaklaşık dört gün elektriksiz kalıyor. 100 tesisin üretim dışı kaldığı uç senaryoda ise şehirlerde ortalama 14 gün boyunca elektrikler kesiliyor. Uç senaryoya göre sistemin yeniden ayağa kaldırılması için gereken süre ise tam 4 hafta, yani yaklaşık bir ay... (enerjigunlugu.net, 2015)

Geliştirilen bu senaryolara göre, siber saldırı sonucu ABD'de oluşacak kapsamlı elektrik kesintinin ABD ekonomisine zararları göz önüne serilmektedir.

Baz senaryoda 250 milyar dolara yaklaşan zarar, uç senaryoda ise bir trilyon doların üzerine çıkıyor. (enerjigunlugu.net, 2015)

Cambridge Üniversitesi Risk Araştırmaları Merkezi ile Lloyd'un ortak çalışmasına göre, siber saldırı sonucu oluşacak elektrik kesintilerinin ekonomik maliyetleri sektörel bazda da analiz ediliyor. Buna göre en büyük zararı, toptan ve perakende ticaret sektörleri görüyor. Oluşacak zararlar listesindeki en büyük ikinci kalemi ise kesintiler sonucu kamu hizmetlerinde yaşanacak aksamaların maliyeti oluşturuyor. Sanayi-üretim sektörü, konaklama ve gıda ile konutlar da siber saldırının en büyük zarara yol açacağı diğer alanlar olarak sıralanıyor. (enerjigunlugu.net, 2015)

Yapılan çalışmaya göre, elektrik şebekelerine yönelik olası bir siber saldırının yol açacağı ekonomik kayıpların sigorta sektörüne çıkaracağı fatura da oldukça ağır. Buna göre sigorta sektörü baz senaryoda 21 milyar doların üzerinde bir teminat ödemesiyle karşı karşıya kalaacak. Üç senaryoda ise bu rakam 70 milyar doların üzerine çıkıyor. (enerjigunlugu.net, 2015)

Dünya genelinde yapılan bu siber saldırıların büyük bir çoğunluğu sistemin eski çalışanları ve aktif çalışan personellerinin yardımı ile yapıldığı görülmektedir. Bu şekilde sistemi iyi tanıyan kişiler kendilerine bırakılan açık kapıları daha iyi bildikleri için bunları kullanmaya çalışırlar. Sonuç ne olursa olsun siber saldırılarda mutlaka bir iz kaldığı için yasalar önünde mutlaka cezai işlem neyse er ya da geç yapılmaktadır. Fakat siber saldırının yapıldığı anda veya sonrasında kuruma, kişilere veya ülkelere verdikleri zararlar oldukça yüksek boyutlara hatta küresel boyutlara erişebilmektedir.

Bu tarz siber saldırıların maddi boyutunun yukarıda belirtilen boyutlara ulaşmaması için en temel kullanıcının bile dikkatli davranması, güvenlik yazılımlarına sahip olması ve bunları güncel tutması, devre dışı bırakmaması gerekmektedir. Malesef en basit kullanıcı hatası bile sistemde ciddi açık kapılar bırakabilir, bu kapıları kullanan saldırganların hayal edebileceklerinden bile daha büyük maddi ve manevi kayıplara neden olunabilmektedir.

Baz senaryodaki 21 milyar dolarlık zarar bile dünyanın gelişmiş ülkeleri arasında bulunan Amerika Birleşik Devletlerini bile sarsacak bir rakam olarak telaffuz edilebilir. Her zaman böyle senaryolarda en kötüsüne bakılması gerektiğini düşünecek olursaş uç senaryoda oluşacak 70 milyar dolar zarar ülkeyi derinden sarsmaya yeter de artar bile...

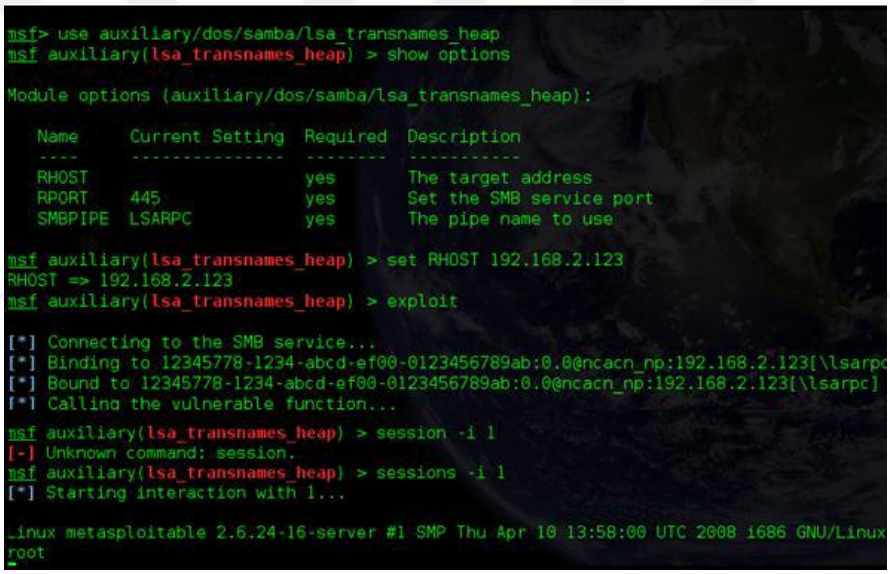
Bu sebepledir ki en temel kullanıcıdan en yetkili kullanıcıya kadar her bir kullanıcının sistemde güvenlik açıklarına olanak verecek kaynağı belli olmayan uygulamaları yüklemekten kaçınmalı, güvenlik önlem ve adımlarını önemsememezlik etmemelidir. Hatta bu saldırının maddi izlerinden çok evinde hasta yatağında elektrikli cihaza bağlı yatan kişinin dört gün yada bir ay sürecek elektrik kesintisine hazırlıksız yakalanabileceği ve bunların sonucunda ölümle burun buruna gelecek sonuç yüzünden vicdani acı boyutunu yaşamamak adına daha dikkatli olmalıdırlar.

Siber saldırıları yaşandıktan sonra engellemek yerine daha yaşanmadan engelleyebilecek güvenlik önlemleri ve uzmanlarıyla kurumun ya da kuruluşların önlem alması ve politikalarını ona göre düzenlemeleri etkili çözüme ulaşmak konusunda fayda sağlayacaktır.

Yapılan saldırı senaryosunun en baz senaryoda bile genel ABD ekonomisine verdiği zarar 250 milyar dolar, uç senaryoda ise 1 trilyon doların üzerine çıkabilme riski bile bazı riskler yaşandıktan sonra değil de yaşanmadan önlem alınmasını gözler önüne sermektedir.

**Senaryo 5: Sunucu Tarafında Yapılan Saldırı Senaryosu**

**Şekil 11.** Linux Sunucuya Sızma Senaryosu




**Kaynak :** (YİĞİT & AKYILDIZ, 2014)

Sunucular üzerinde çalışan servislerde, fuzzing gibi sıralı veri göndererek sistemin kendi yapısından kaynaklı hataları bulabilen test yöntemleri vu buna benzer yöntemler kullanılarak bulunan ve sızma kodları yazılan sıfırıncı gün açıklıkları ya da bilinen diğer açık noktalar bulunabilmektedir. Sunucuların sürekli olarak güncel tutuluyor olması bile sıfırıncı gün açıklıklarını engelleyemese de bilinen açıklıkların kapatılması için hayati önem taşımaktadır.

Şekil 11'de ise vsftpd servisi kullanan Linux işletimi sistemi buffer overflow açıklığından faydalanılarak ele geçirilmesi gösterilmiştir. (Yiğit & Akyıldız, 2014)

- Senaryo 6: İlk Devlet Ölçekli Modern Siber Saldırı - 2007 Estonya

Ülkeler siber dünyaya adım attıkça siber saldırganlarınında dikkatini çekmeyi başardılar. Yapılan her yeni hizmet halka kolaylık sağlasa da başlarda ülkelerin pekte görmediği ya da ciddiye almadığı siber güvenlik kavramı konusunda önemli adımlar atılması gereğini ortaya koymuştur.

Dünyada yaşanan soğuk ve sıcak savaş dönemlerinin aksine artık yeni bir kavramda ülke gündemlerine oturdu. Artık siber saldırı atakları da ciddi anlamda ülkeleri tehdit etmeye başladı.

2007 yılında Estonya devletine, özel ve kamu kuruluşlarına yapılan toplu siber saldırı atakları bu konuda karşılaşılan modern dünyanın yeni bir gerçeği olarak karşımıza çıkmıştır.

Estonya kamu kurum ve kuruluşlarına, haber ajanslarına, devlet başkanının internet adresine, bankacılık adresleri gibi yerlere yapılan bu saldırının yapım metodu DDoS saldırıları ile gerçekleştirilmiştir.

Estonya 1991 yılında kurulmuş olmasına rağmen teknolojik yatırım ve programları sayesinde teknolojik olarak üst düzey noktalara hızlı ulaşmıştır. Örnek verecek olursak Skype'ın hazırlanmasında kullanılan yazılım, Estonya menşeiliydi. Dünyada ilk defa 2005 yılında Estonya devleti elektronik oy kullanarak seçim gerçekleştirme imkânını vatandaşlarının hizmetine sunmuştur.

Bu dönemde artık halkın yüzde 60'a yakını günlük ihtiyaçlarının önemli bir kısmında internete muhtaçtı. Ülkedeki bankacılık işlemlerinin yaklaşık yüzde 96'sı internet üzerinden gerçekleştiriliyordu. Dolayısıyla her vatandaşın devlet kurumlarına ve bankalarına internet üzerinden bağlanmasına imkân veren bir dijital kimliğe sahip olduğu ülkede, 355 devlet kuruluşu sanal dünyada yer almaktaydı. (Yazıcı, 2015)

X-Road sistemini çökertmek için özel olarak düzenlenmiş veri paketlerinin yönlendiricilere gönderildiği bu saldırılar sırasında DDoS (dağıtık servis dışı bırakma saldırısı) ile pek çok ülkeden gelen IP adresleri kaydedilmişti. Saldırılara karşı önlem olarak Estonya hükümeti bant genişliğini; özel kuruluş ve firmalar da sunucularının

sayısını ve alan genişliğini artırdı. Yine de zor durumda kalan Estonya Savunma Bakanı Dr. Jaak Aaviksoo NATO'ya ve diğer ülkelere yardım çağrısında bulundu. (Yazıcı, 2015)

Saldırıların hedefleri ise devlet kurumlarının pek çok kademesini içermekteydi: Estonya Başkanlığı ve Parlamentosu, neredeyse tüm ülkedeki devlet bakanlıkları, siyasi partiler, 3 büyük haber kuruluşu, iletişim firmasının yanı sıra *Hansabank ve SEB* gibi bankalar sonuç olarak siber saldırılara maruz kalmıştı. Saldırının yol açtığı hasar tam olarak belirlenemedi. (Yazıcı, 2015)

Estonya'ya karşı yapılan siber saldırılar, NATO'nun siber güvenliğe bakışının şekillenmesinde önemli rol oynadı. NATO'nun Yeni Güvenlik Tehditleri Bölümü'nden sorumlu NATO Genel Sekreter Yardımcısı Büyükelçi Sorin Ducaru, Washington'da yaptığı açıklamada "Estonya, NATO'nun bu alandaki ilk politikasını oluşturmada tetikleyici bir rol oynadı. Siber saldırıları Gürcistan'daki savaşta, Ukrayna savaşında ve de Kırım referandumu öncesi net bir şekilde gördük. NATO sadece yüksek seviyedeki değil, veri şifrelemesinden siber suça kadar birçok alana bakıyor. Bununla birlikte siber alanda ciddi derecede kesintiye uğratma veya imha etme tehlikelerine karşı da çalışmalar yapıyor" diye konuşmuştu. (Yazıcı, 2015)

NATO, kendi birimindeki en iyi siber-terörizm uzmanlarını Tallinn'e sevk etti. Alanda araştırma ve ülkenin elektronik savunma sistemlerini güçlendirici çalışmalar yapıldı. NATO'nun 1999 Sırp bilgisayar korsanlarının saldırısı sonrasında artarak büyüyen siber güvenlik ilgisi Estonya'nın uğradığı saldırılar sonrasında gözle görünür hale geldi. (Yazıcı, 2015)

Yapılan saldırıların maddi boyutu anlaşılamasada devletlerin siber güvenlik alanında yeni stratejiler belirlemesi ve bununla ilgili organları ivedilikle oluşturmasına öncülük etmesi açısından önemli sonuçlar doğurmuştur. Bu sayede devletlerin siber saldırılara karşı farkındalıkları artmış olması açışından da dünyayı bu anlamda da yönlendirmiştir.

- Senaryo 7: Son Kulluanıcıya (Client) Yapılan Saldırı Senaryosu

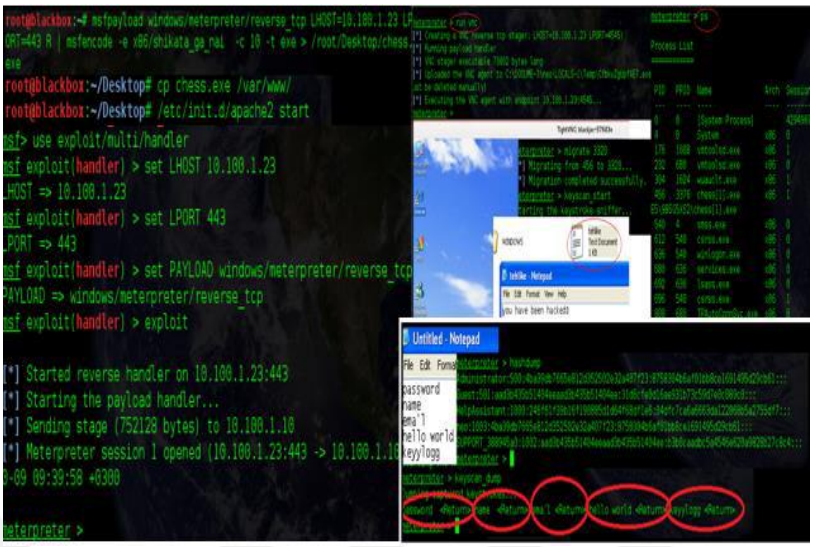
Son kullanıcının bilgisayarına veya sistemie sızmak kaydı ile siber saldırı düzenlemekte oldukça sık başvurulan bir yöntemdir. Son kullanıcılar tarafından

bilgisayarlarına indirilen müzikler, oyunlar, pdf dosyaları, yazı veya sunum dosyaları, flash tarzı küçük oyunlar, güvenilmeyen kaynaklardan indirilen çeşitli dosyaların içerisine gizlenen kötü amaçlı yazılımlar sayesinde son kullanıcı (client) tarafında söz konusu bu programın çalıştırılması sayesinde bilgisayarınıza yüklenerek aktif hale gelirler. Bu kötü amaçlı dosyalar antivirüs ve düzgün yapılandırılmamış güvenlik duvarları, kullanıcı hataları, sosyal mühendislik, toplu e-posta saldırıları, yemleme gibi yöntemler sayesinde bilgisayara veya sistemlere sızmayı başarırlar. Kötü amaçlı yazılım sayesinde sisteme sızan istenmeyen üçüncü kişiler sistemde her istediği bilgiye ulaşabilmek için her türlü yolu deneyeceklerdir.

Örneğin Şekil 12'de dışarıdan bakıldığında satranç oyunu gibi gözüken kötü amaçlı yazılım son kullanıcıya (client) gönderilmiştir. Son kullanıcınında içinde kötü amaçlı yazılım olduğunu bilmeden çalıştırdığı bu satranç oyunu görünümlü program bilgisayarda istinilen bilgilerin sızdırılması amacı ile programın yüklendiği anda aktif hale gelecektir.

Son kullanıcının bu dosyayı açmasıyla bilgisayarının ele geçirilmesi Şekil 12'de gösterilmiştir. Son kullanıcının sistemine, yeni bir kullanıcı eklenilerek ekran görüntüsü alınabilmiştir. Ayrıca son kullanıcının bilgisayarında tuş kaydedici (keylogger) program çalıştırılarak bastığı tüm tuşlar görüntülenmiştir. (Yiğit & Akyıldız, 2014)

**Şekil 12.** Son Kullanıcı Yapılan Saldırı Senaryosu




**Kaynak :** (YİĞİT & AKYILDIZ, 2014)

- Senaryo 8: Küresel APT Saldırı Senaryosu

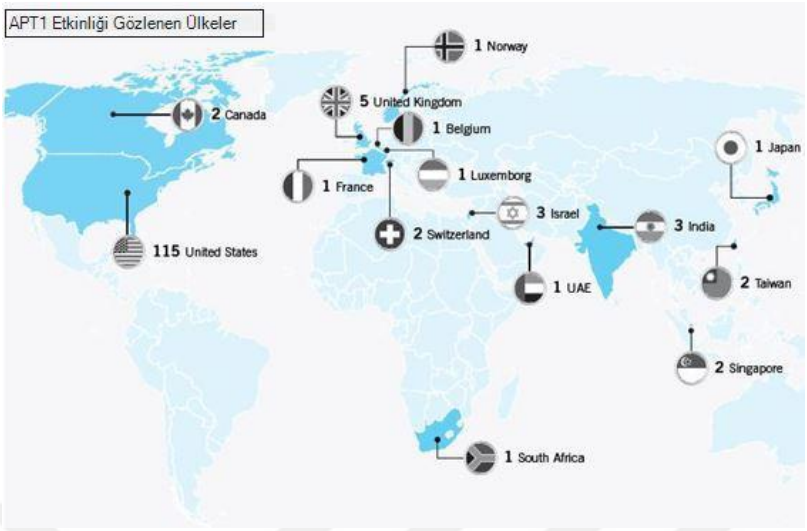
Amerikan siber güvenlik firması Mandiant'ın Şubat 2013'te yayınladığı rapora göre, yaşanmış APT saldırılarından biri olan raporda APT1 adını verdikleri siber saldırı oldukça vahim sonuçlar doğurmuştur.

Raporda Çin Halk Cumhuriyeti'nin 20'den fazla APT saldırı grubundan biri olarak adlandırdığı APT1 grubu küresel anlamda birçok devlete ve kuruma sızmış aylarca hatta yıllarca sistemde kalıp veri kopyalamayı başarabilmişlerdir.

Raporda belirtildiği üzere Mandiant 2006-2013 yılları arasında APT1 grubunun 20 ana sektörde 141 firmaya sızdığını ve yüzlerce terabayt veri çaldığını tespit etmiştir. Bu grubun sızdığı kurbanlarının ağında ortalama 356 gün kaldığı belirtilmiştir. Ayrıca en uzun süre kaldığı kurbanın ağında ise 4 yıl 10 ay süre ile kaldığı tespit edilmiştir. (Özbay, 2015)

APT1 saldırısında hedef olan ülkeleri Şekil 13'te görebilirsiniz. Şekilden de anlaşılacağı üzere özellikle İngilizce dilini kullanan veya İngilizce anadil olarak işletim sistemi işaretli olan bilgisayar sistemlerine saldırı düzenlendiği görülmektedir.

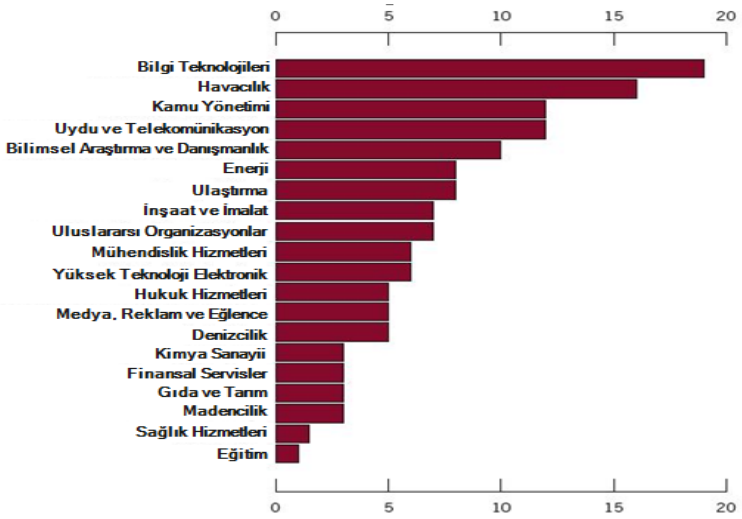
**Şekil 13.** Apt1 Saldırısının Sızdığı Ülkeler




**Kaynak :** (ÖZBAY, 2015)

Gelişmiş siber saldırıların ve özellikle APT saldırılarının daha zor tespit edildiği ve daha az iz bırakıldığı için devletler arası siber savaşta yaygın olarak kullanıldığı düşünülmektedir. Mandiant siber güvenlik firmasının hazırlamış olduğu APT1 raporunda kurbanların sektörlere göre dağılımına bakıldığında saldırı boyutunun bireyselden daha büyük bir ölçeğe sahip olduğu gözlemlenebilir. Şekil 14'te ise hedefte olan sektörleri ve bunların içerisinde kaç organizasyona sızıldığını görebiliriz.

**Şekil 14.** Sektörlere Göre Apt1 Saldırısının Sızdığı Firma Sayısı



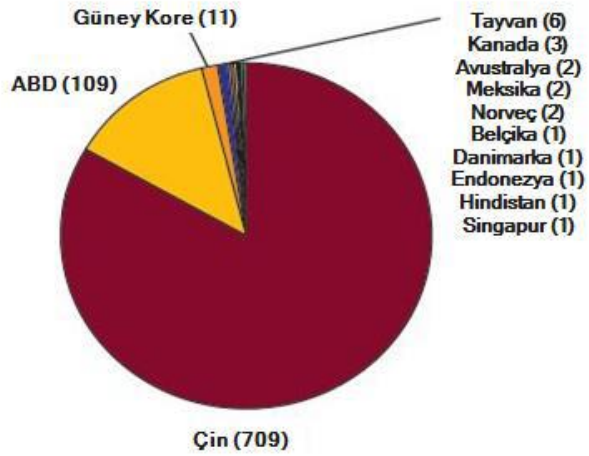

**Kaynak :** (ÖZBAY, 2015)

Raporda APT1'in sızdığı kurbanlarından çok fazla veri çalındığı belirtilmektedir. Ne tür veriler çalınmış diye detaya inildiğinde ürün geliştirme, sistem tasarımı, test sonuçları, üretim süreçleri, standartlar, iş planları, politik analiz dokümanları, üst düzey kişilerin e-postaları ve kullanıcı bilgileri gibi birçok türde veri çalındığı görülmektedir. Bu bilgilerin birçoğu sıradan bir saldırganın eline geçse çok fazla bir şey ifade etmeyecektir ya da bunu parasal değere çevirmesi çok kolay olmayacaktır. Bundan dolayı da gelişmiş siber saldırılan devlet destekli olduğu düşünülebilir. Sadece tek bir firmadan 10 aydan fazla sürede 6,5 terabayt veri çalındığı belirtilmiştir. Bundan dolayı da saldırılar toplamında yüksek miktarda veri çalındığı tahmin edilmektedir. (Özbay, 2015)

Mandiant'ın hazırladığı siber güvenlik raporunda vurguladığı bir diğer husus ise APT1'nın kurbanlarına doğrudan bağlanmak yerine vekil sunucular (Proxy server) kullanarak bağlandığı ve bu sunucuların farklı yerlerde bulunduğudur. Gelişmiş siber saldırıların tespit edilmesi ve pasif sistemlerle engellenmesinin önündeki zorluklardan biri de saldırının farklı farklı ülkeler üzerinden gerçekleştiriliyor olmasıdır.

Şekil 15'te, APT1 grubunun sunucuları ve hangi ülke üzerinde kaç tane olduğu belirtilmiştir.

**Şekil 15.** Doğrulanmış Apt1 Sunucularının Ülkelere Göre Dağılımı




**Kaynak :** (ÖZBAY, 2015)

Şekil 15'te belirtilen saldırı sunucuları herhangi biri ya da birden fazlası bulunmuş ve engellenmiş olsa bile malesef kurban siber saldırıdan kurtulamamakta diğer sunucular engellenen sunucuların yürütmüş olduğu saldırıya kaldığı yerden devam edeceklerdir. Bu sebeple büyük ölçekli siber saldırılardan korunmak için bireysel çabalar yerine siber güvenlik uzmanlarınca alınan önlemler daha etkili bir yol olacaktır.

Düzenlenen bu siber saldırının sonucunda izinsiz kopyalanan binlerce terabaytlık veriler bireysel kullanıcılar açısından bir anlam ifade etmese de devletler veya büyük kuruluşlar için önemli siber casusluk ve sanayi casusluğu açısından önem arz etmektedir. Geliştirilecek yeni teknolojinin patenti alınmadan bu saldırıyla elde edilmesi haksız olarak bilgiyi hırsızlığı yapan kuruluş tarafından hakkı olmadığı halde ürünü adına kaydettirme, patent hakları, izinsiz satış işlemleri gibi ciddi maddi kayıplara neden olabilecektir.

- Senaryo 9: Yemleme (Phising) Saldırı Senaryosu

Yemleme (Phising) adı verilen son kullanıcı tarafında yapılan saldırılarda ise son kullanıcıları kandıracak e-posta ya da mesajlar atarak farkında olmadan kullanıcın kendi elleriyle şifre, kişisel bilgi, kurumsal bilgi veya bankacılık işlemlerinde kullandığı şifreler gibi bilgileri yazması yoluyla bilgiler ele geçirilir. Daha sonrasında bu bilgilerle siber saldırganlar kredi kartı ve bankacılık işlemleri dolandırıcılığı, kurumsal veya

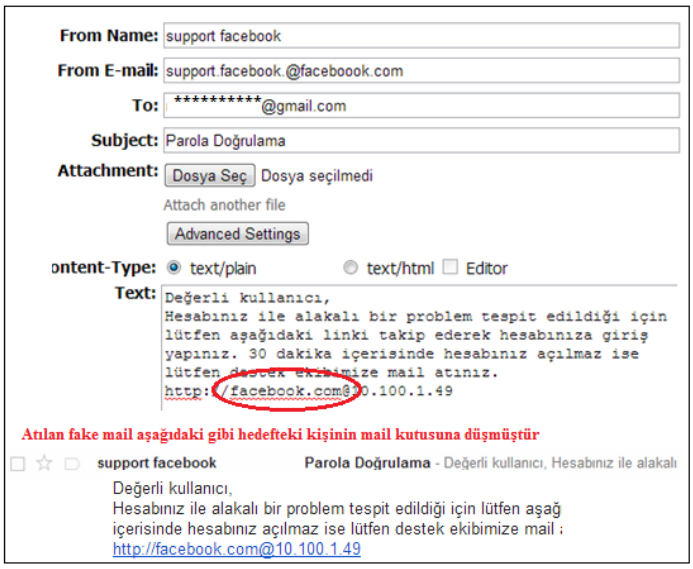
kişisel bilgi hırsızlığı gibi işlemler yaparak son kullanıcıyı bazen geri dönülemez maddi ve itibar kaybı gibi manevi zararlara uğratabilirler.

Yemleme saldırıları özellikle dikkatsiz son kullanıcılar ile teknik olarak sisteme ve bilgisayara daha az hakim olan son kullanıcıları hedef almakta ve bu kişilerin yapılan bu yemleme saldırısı tuzağına düşmesi çok daha kolay olmaktadır. Şunu unutmayın ki hiçbir kamu ya da özel kurum - kuruluşlar asla ama asla sizden e-posta yoluyla şifrenizi ve kullanıcı bilgilerinizi istemezler. Size atılan fake denilen sahte mail gerçek kuruluşun birebir benzeri olan siteye sizi yönlendirir, siz de sanki o siteymiş gibi siteye giriş (login) yapmak için ilgili yere tıklayıp girmeye çalıştığınızda bütün bilgi ve şifrenizi ellerinizle istenmeyen kişilere vermiş olursunuz. Esas sorun bu aşamadan sonra başlar ki, o da kötü niyetli siber saldırganının insafına kaldığınızdır. Bu konuda da bu kişinin insaflı davranacağını beklemek pekte akıllıca olmaz.

Yapılan yemleme saldırıları özellikle bankacılık şifrelerinizi içeren bilgilerinizi elde etmek için kurulmuş bir tuzaksa ve kredi kartı limitiniz yüksek ve boşsa işte o zaman saldırgan alışveriş yapmak, para çekmek, havale ve eft yapmak gibi yöntemlerle size ciddi anlamda büyük maddi kayıplar verebilir.

Eğer ki kurumsal kullanıcı adı ve şifrelerinizi yemleme saldırılarıyla kopyalattıysanız o zaman tehlike hem maddi hem manevi anlamda daha büyük olmaktadır. Manevi anlamda şirketinizin ya da kurumunuzun saldırıdan dolayı toplum önünde küçük düşmesi veya siber saldırganın kasıtlı olarak uygunsuz işler yapması ve paylaşması dolayısı ile itibarının önemli ölçüde zedelenmesi olasıdır. Maddi kayba gelecek olursak, müşterilerinizin kişisel bilgi ve belgeleri topluma ifşa edilebilir yada rakip kuruluşlara, sanayi casusluğu yapılarak projelerinizin teknik içeriği yine rakip işletmelere ya da topluma ifşa edilmek sureti ile projeleriniz tamamen değersizleşebilir ya da kısmen değer kaybedebilir.

**Şekil 16**. Yemleme E-Posta Saldırı Senaryosu




**Kaynak :** (YİĞİT & AKYILDIZ, 2014)

Şekil 16'da örnek bir yemleme e-posta'sı oluşturulmuştur. Bu senaryoda internet üzerinden sahte e-posta atılabilen bir siteden yararlanılmıştır. Şekil 16'da http://facebook.com@10.100.1.49 adresi facebook sitesine yönlendirmesi gerekirken adres son kullanıcıyı @ işaretinden sonraki IP adresine yönlendirecektir. Son kullanıcı linke tıkladığı anda sahte sayfaya yönlendirilecek şifreleri çalınma riskiyle karşı karşıya kalacaktır. (Yiğit & Akyıldız, 2014)

- Senaryo 10: APT30 Saldırı Senaryosu

FireEye tarafından yayınlanan raporda yoğun olarak Güneydoğu Asya ve Hindistan'ı hedef aldığı belirtilen grup APT30 olarak adlandırılmıştır. (Özbay, 2015)

Düzenlenen APT30 saldırıları ile grup üyelerinin on yıl gibi uzun bir süreye yayarak saldırı yapılan bölgedeki devlet kuruluşları ve ticari kuruluşların internet ve intranet ağlarına sızdıkları görülmüştür.

Grup üyeleri basit saldırılardan ziyade daha karmaşık bir yapıda saldırı planlaması gereken internet bağlantısı olmayan ağ bağlantısı olan intranet bağlantılarından izinsiz veri kopyalamaya odaklanmıştır. Bu tip bir saldırıda ama amaç büyük maddi kayıplar verdirmek yerine saldırıyı on yıl gibi uzun bir zamana yayarak farkedilmeden sistemde kalıp mümkün olduğu en büyük boyutta veriyi istenmeyen

üçüncü kişilere sızdırmak amaçlanmıştır. Bu saldırıda grubun aktiviteleri izlendiğinde ve kullanılan araçlara bakıldığında hedeflerinde siyasal, askeri ve finansal verileri kopyalamak olduğu anlaşılmıştır. Bu saldırılar standart saldırı tiplerinin aksine acemi düzey ya da orta düzey siber saldırganlar yerine daha konunun uzmanı siber saldırganlar tarafından yapıldığı aşikardır. Çünkü interneti olmayan bir ağa sızmak çok daha zor ve karmaşık algoritma ve araçlar kullanmayı gerektirir, kaldı ki sistemde on yıl boyunca onca güvenlik duvarı ve aktif güvenlik yazılımına yakalanmadan kalabilecek araç gerek geliştirmekte konunun uzmanları tarafından planlandığını ve gerçekleştirildiğini göstermektedir.

Diğer saldırı tiplerinin aksine APT30 saldırısında grup üyeleri hızlıca verileri kopyalayıp mümkün olduğunca bu işi çabuk yapmak yerine işi aceleye getirmeden on yıl gibi uzun bir sürede sistemde kalarak yavaş yavaş ama olabildiğince çok veriyi siber saldırganlara izinsiz olarak ulaştırmayı hedeflemişlerdir.

Esasına bakıldığında gelişmiş siber saldırıların düzenlenmesindeki amaç, düşük ekonomik kazanç sağlamak ya da kitlesel ses duyurma gibi hedeflerden çok kişilerden ziyade devletler için önem arz eden yüksek oranda veri kopyalamak vardır. Bu sebeple karmaşık yapıda düzenlenmiş olan bu saldırılar karşısında pasif savunma sistemleri tek başına yeterli gelmemektedir.

Yapılan bu APT30 saldırılarının sonucunda Güneydoğu Asya ve Hindistanın devlet kuruluşları ve saldırı mağduru diğer kuruluşlaından yıllar boyu çekilen yüksek orandaki veri yüzünden ciddi bilgi ve teknoloji hırsızlığı sonucu doğmuştur. Bu sebeple ülkelerin güvenlik yaazılımlarını tekrar elden geçirme ve gerekli yamalar ve programlarla desteklemesinin önemini yetkililer yaşayarak tecrübe etmişlerdir. Bu sorun aslında çağımızın en ciddi sonuçlarını doğurmuş ve bilgi güvenliğinin önemi gün geçtikçe daha iyi anlaşılmıştır.

- Senaryo 11: Türkiye'ye Karşı Bankshot İle Yapılan Siber Saldırı Senaryosu

8 Mart 2018 tarihinde, Kuzey Kore temelli bir grup olduğu düşünülen “Lazarus Grup” (bir diğer adı ile “Hidden Cobra”) isimli “Siber Suç Örgütü”nün Türkiye'deki finans sistemine yönelik düzenlelediği siber saldırılar deşifre edilmiştir. Düzenlenen bu saldırılarda, grubun en son faaliyet tarihi olarak 2017 yılında görülen “Bankshot” zararlı yazılımının daha da geliştirilmiş sürümü ile geri dönüş yaptığı bilinmektedir.

Bankshot yazılımı, kurbanından daha fazla bilgi elde edebilmek için kurbanın ağına yerleşmek üzere özel olarak tasarlanmış bir zararlı yazılım olarak değerlendirilebilir. Toplanan veriler ile saldırganların kurbanları ve yaptıkları işlemler hakkında bilgi toplamak için söz konusu zararlı yazılımı kullanarak ülkemizin finans sektörünün bağlı olduğu sistemlere yönelik, hedef odaklı bir operasyon planlayabileceği ihtimalini göz ardı etmemek gerektiğini bizlere hatırlatmıştır.

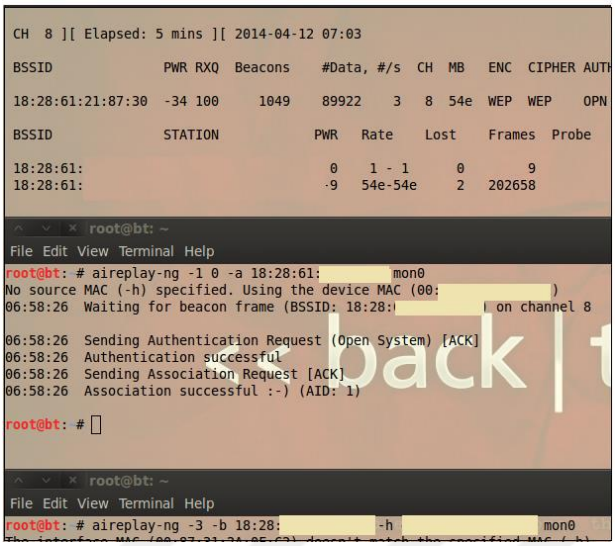
Türkiye'deki finans kuruluşlarına düzenlenen bu siber saldırıda asıl hedefin muhtemelen diğer ülkelerden gelecekteki olası soygunlar için erken veri toplama aşamasının ne olabileceği kaygısı oluşmuştur. Kurbanın sistemlerine almak için yakın zamanda sıfır gün süren bir Adobe Flash güvenlik açığından yararlanıldığını düşünülmektedir.

Hedefteki Türk kuruluşları virüslü dosyalarının 'oltalama' yöntemiyle Microsoft Word ekli e-postalar aracılığıyla yayıldığı bildirildi. Euronews'ta yayınlanan haberde virüslü dosyaların kullanıcıları Bitcoin satın almaya yönlendirdiği iddiası yer aldı. (siberbulten.com, 2018)

- Senaryo 12: Kablosuz Ağ Saldırı Senaryosu

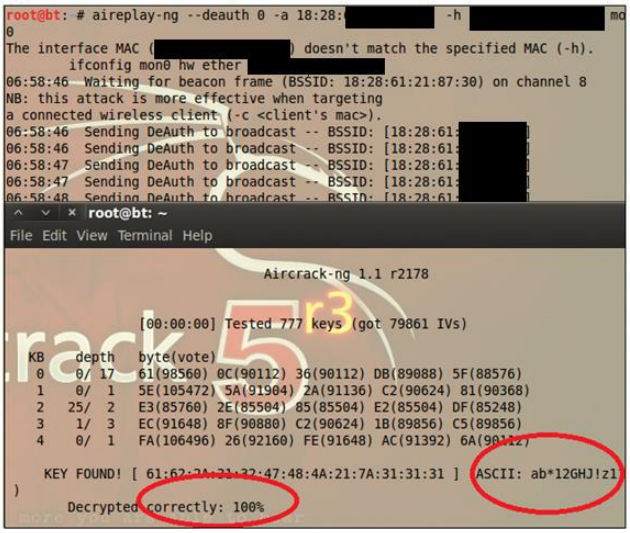
WEP şifreleme yöntemi ile yapılan kablosuz ağ şifrelemeleri kullanılan algoritmalarla artık oldukça kolay bir şekilde kırılabilmektedir. Gökkuşağı tablosu ya da gökkuşağı başvuru çizelgesi (Rainbow Table) yöntemini kullanılarak WPA ve WPA2 şifrelerini de kırabilmek mümkündür. WPA ve WPA2 şifreleme yöntemi WEP yöntemine göre daha gelişmiş ve kırılması daha zor yöntemler olsa dahi eğer ki kullanıcı basit ve ardışık karakterlerden oluşan şifre kullanırsa bunları kırmak çok daha kolay olabilecektir. Bu sebeple hangi şifreleme algoritması ya da yöntemini kullanırsanız kullanın mutlaka karmaşık ve bulunması daha zor karakterler kullanarak şifre oluşturun.

**Şekil 17.** Sahte Doğrulama Paketi




**Kaynak :** (YİĞİT & AKYILDIZ, 2014)

**Şekil 18.** Wep Yöntemiyle Oluşturulan Şifreyi Kırma




**Kaynak :** (YİĞİT & AKYILDIZ, 2014)

Şekil 17 ve 18'de kademeli olarak WEP şifresi kırılmıştır. Ağ kartı monitor moda alınarak havadaki tüm kablosuz yayınların görüntülenmesi sağlanmıştır. Airodump-ng aracı kullanılarak monitor edilen kablosuz ağ trafiği Şekil 17'de gösterildiği gibi yakalanmıştır. 50000 civarında yada daha fazla paket toplanarak , toplanılan paketler ile WEP şifresinin kırılması planlanlanmıştır. Burada, sahte

doğrulama paketleri gönderilerek authentication ‘opn’ durumuna getirilir. Daha sonra arp reply paketleri enjekte edilerek toplanılan paket sayısı arttırılır. Son olarak aircrack-ng aracı ile WEP şifresi Şekil 18’deki gibi kırılmıştır. (Yiğit & Akyıldız, 2014)

- Senaryo 13: Uygulama Alanında Yapılan Saldırı Senaryosu

Yazılan uygulamaların kodlarının genellikle gereğinden fazla uzun olması, kullanıcıların dikkatsiz ve özensiz davranması, çalışanların veya kullanıcıların kalifiye olmaması gibi bazı durumlardan dolayı uygulama tabanında oluşan integer, string ve blind sql injection açıklıkları oluşabilmektedir. Bu durumu örneklendirecek olursak eğer SQL sorgularının filtrelenmeden sisteme alınmasından dolayı herhangi bir sisteme ait olan veritabanını ele geçirmek mümkündür.

DWVA simülasyon programında yapılan saldırı sonucunda Şekil 19’da gösterildiği gibi veri tabanından tablolar çekilmiştir. (Yiğit & Akyıldız, 2014)

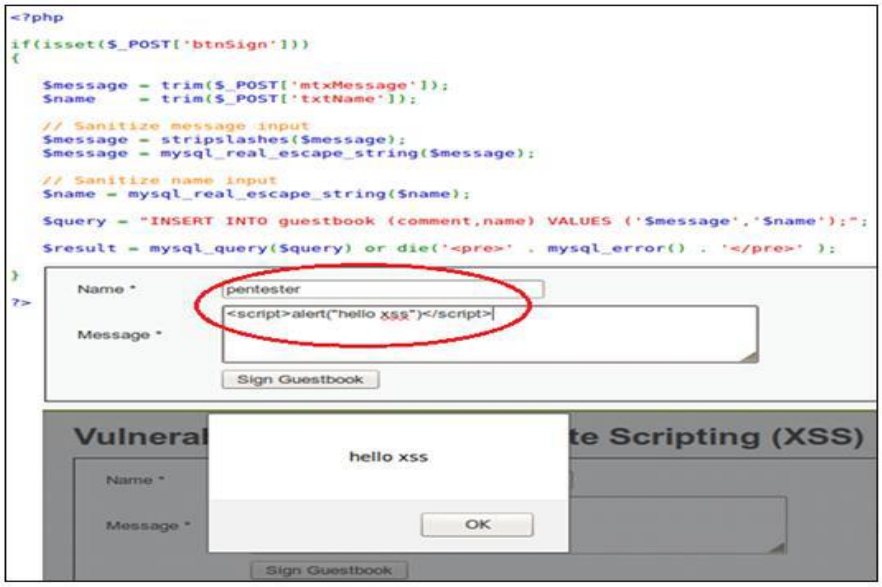
**Şekil 19.** Sql Injectıon Saldırı Senaryosu




**Kaynak:** (YİĞİT & AKYILDIZ, 2014)

Şekil 20’de kaynak kodlardan XSS açıklığı olduğu çok rahat görülebilmektedir. XSS açıklığının olduğu kutunun içerisine yazılan javascript kodları ile bu açığın olduğu gösterilmiştir. (Yiğit & Akyıldız, 2014)

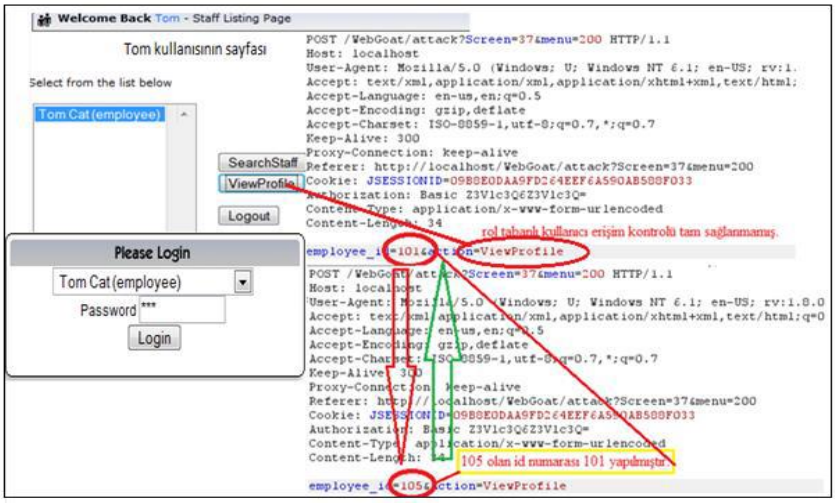
**Şekil 20.** Xss Açıklığı Saldırı Senaryosu




**Kaynak :** (YİĞİT & AKYILDIZ, 2014)

Yetkilendirme hatalarından dolayı oluşabilecek bir açıklıkta Şekil 21'de gösterildiği gibi istismar edilmiştir. Burada kullanıcı kaydolurken yetki kontrolü yapılmıştır. Kullanıcı kaydolduktan sonra belirli kişilerin profillerini görüntülemeye yetkili olmasına rağmen, saldırı yapan kişi yaptığı istekleri Burp Suite aracı ile keserek kendi ID numarası ile yönetici kullanıcısının ID numarasını değiştirerek görmeye yetkili olmadığı bilgileri görüntüleyebilmiştir. (Yiğit & Akyıldız, 2014)

**Şekil 21.** Yetkilendirme Açıklığı Saldırı Senaryosu




**Kaynak :** (YİĞİT & AKYILDIZ, 2014)

- Senaryo 14: Ağ Fidye Yazılımı Saldırı Senaryoları

Marriott ve Facebook gibi şirketler içerik izni olarak haberlere izin vermesiyle siber güvenlik saldırıları dünya genelindeki bu büyük kurumları, ağ fidye yazılımı (ransomware) ihlallerine bağlı kabuslar yaşatmaya itmiştir. Ransomware, bir miktar para ödenene kadar bir bilgisayar sistemine erişimi engellemek için tasarlanmış bir tür kötü amaçlı yazılımdır ve hızla çevrimiçi saldırıların en popüler biçimlerinden biri haline gelmektedir.

Siber Güvenlik Girişimleri'ne göre, AIDS Trojan saldırısı ile 1989'dan başlayarak, fidye yazılımları büyük ölçekte gelişiyor ve 2021 yılına kadar yıllık 20 milyar doların üzerinde bir dolandırıcılık maliyetine sahip olması bekleniyor. (Price, 2019)

Fidye yazılımı saldırılarını önlemek için kuruluşların ağ güvenliğini birinci öncelik haline getirmesi gerekir. Siber güvenlik ihlallerini ortadan kaldırmanın ilk adımı, virüsten koruma ve kötü amaçlı yazılımdan koruma yazılımlarını dağıtmaktır. Ağı daha fazla korumak için kuruluşlar erişim denetimini belirli düzeylerde kısıtlayabilir. Örneğin, Amerika Birleşik Devletler Bilgisayar Acil Durum Hazırlık Ekibi (US-CERT), erişim denetimlerinin (dosya, dizin ve ağ paylaşım izinleri) en az ayrıcalık göz önünde bulundurularak yapılandırılmasını önerir. Başka bir deyişle, yalnızca belgeleri, dosyaları vb. okumak için erişime ihtiyaç duyan kullanıcıların bu

belirli dosyaları, dizinleri veya paylaşımları düzenlemesine izin verilmemelidir. Bu sayede alınan önlemlerle ağ fidye yazılımı saldırılarından korunmuş olursunuz.

Siber güvenlik açısından değerlendirdiğiizde yıllık 20 milyar doların üzerinde maddi kayıp içerebilen bir düzeye ulaşması şirketleriniz ve kişisel kayıplarınız açısından siber güvenlik önlemlerini ne kadar sıkı tutmamız gerektiğinin önemli bir kanıtı olarak karşımıza çıkmaktadır.

- Senaryo 15: Yan Kanal Saldırı Senaryosu

Yan kanal saldırıları sistemlerin güç analizine, elektromanyetik uygulamalarına ve zamanlanmış görevlerine yönelik saldırılardır. (Yılmaz & Sağıroğlu, 2013)

Bu saldırıların yapılmasındaki esas amaç şifreleme anahtarını ele geçirecek bir casus uygulamayı sisteme sızdırmaktır. Çoğu akıllı sistem ve akıllı teknoloji maalesef bu saldırıların sonucunda sistemde kayıtlı olan müşteri bilgilerini, kişisel kullanım bilgilerini ve şifrelerini kaybetmesine neden olabilmektedir.

Bu yapılan saldırı sonucunda kullanıcı bilgileri ticari şirketlere reklam amaçlı satılabilir ve bu yüzden rahatsız edici mesajlara ve e-postalara maruz kalabilirler. Kopyalanan şifreler ile maddi kayıplar verilen dolandırıcılık, şirketin gizli bilgilerinin ifşa edilmesi, ticari itibar kaybı gibi maddi anlamda ciddi kayıplar verebilirler. Kişisel kullanım bilgileri de aynı şekilde şirketlere satılarak ticari reklam içeren mesajlar ve e-postaların gönderilmesi yoluyla kullanıcı manevi olarak rahatsız edilebilir. Artık ülkemizde bunlar suç kapsamında sayıldığı için istenmeyen reklam postası veya mesajı almamak mümkün olmaktadır fakat yine de kullanıcının üye olmadığı yerlerden mesajlar gelerek kullanıcılara rahatsızlık verecek aşamaya gelebilir.

Görüldüğü üzere istenmeyen sonuçlar manevi ve maddi açıdan kullanıcıları oldukça zor bir duruma düşürebilir ya da taciz boyutunda ciddi rahatsızlıklara neden olabilmektir.

- Senaryo 16: Bulut Güvenliği Saldırı Senaryoları

Hiçbir kuruluş veri ihlallerine karşı tamamen güvenli değildir. Siber güvenlik kavramı her gün kendini yeni saldırı tiplerine göre güncellemektedir. Perakende ve toptan satış şirketleri ve Anthem gibi sağlık sigortası şirketleri daha önce müşteri verilerine yönelik siber saldırı ihlalleri yaşarken, siber güvenlik ihlallerine hedefi olma

korkusu sanal dünyayı aktif kullanan her şirket ve kişide her zaman en üst seviyede olmalıdır. Birçok işletme, bilgisayar korsanlarının verilere erişmesini önlemek için hassas verileri bulutta güvenceye alma eğilimindedir.

Ancak bulut birçok kişi için güvenli bir yol olmaya devam ederken, Gartner 2020'ye kadar bulut güvenliği hatalarının yüzde 95'inin müşterinin hatası olacağını öngörüyor. (Price, 2019)

Kuruluşunuzun başka bir istatistik olmasına asla izin vermeyin. Müşterilerinizi korumak için siber güvenlik önlemlerini mutlaka alın. Fiziksel konum, bilgi işlem cihazı, ağ veya veritabanı gibi bir kaynağa erişmeye çalışan bireyin kimliğinin daha yüksek derecede güvencesini sağlayan Çok Faktörlü Kimlik Doğrulama (MFA) uygulayın. MFA, yetkisiz bir kullanıcının hassas verilere erişimini daha karmaşık hale getiren çok katmanlı bir kimlik doğrulama işlemi oluşturarak güvenli bağlantıyı sağlamayı amaçlamaktadır.

Şifreleme, verileri yetkisiz kullanıcılar tarafından okunamayan anlaşılmaz metne dönüştürerek, müdahalenin ve verilerin tehlikeye atılmasını zorlaştırmaya çalıştığı için güvenlik ihlallerini önlemenin de anahtarıdır. Bununla birlikte, tüm veri şifreleme çözümleri bir ve aynı değildir, bu nedenle verileri beşikten mezara kadar korumak için uçtan uca şifreleme kullanan bir sisteme yatırım yapmak önemlidir, böylece yalnızca gönderen ve alıcı bilgileri yetkilendirebilir.

Bir işletme, güvenli ağ erişimi sağlayan ve tüm iletişim ve kimlik doğrulama prosedürlerinin şifrelenmesini sağlayan en üst düzey güvenlik çözümlerine yatırım yapsa bile, hassas veriler bilgisayar korsanları için risk altında olabilir. Örneğin, gün boyunca iş e-postalarına erişmek için bir cihazı evden (tablet gibi) ofise getirmeye karar veren bir çalışanı düşünün. Tablet, güvenli yazılım veya antivirüs koruması ile kurulamayabilir, böylece güvenli olmayan bir ağa bağlanma riskiyle karşı karşıya kalabilir. Bu türden düzinelerce hatta yüzlerce güvenli olmayan cihazın kuruluşunuzun ağına bağlı olması ve buluta erişmesinin kabusu olduğunu düşünün.

Ponemon Institute tarafından yakın zamanda yapılan bir araştırma, üst düzey yöneticilerin sadece yüzde 35'inin çalışanların veri güvenliği risklerinin kuruluşlarını nasıl etkilediği konusunda bilgili olmasını sağlamanın bir öncelik olduğunu düşündüğünü ve yüzde 60'ı çalışanların bilgili olmadığını veya şirket hakkında hiçbir

bilgiye sahip olmadığını söyledi. Çalışma ayrıca, ankete katılan şirketlerin yarısından fazlasının (yüzde 55) kötü niyetli veya ihmalkâr bir çalışan nedeniyle zaten bir güvenlik olayı yaşadığını ortaya çıkarttı. (Price, 2019)

Birçok organizasyonda, kendi cihazınızı getirin (BYOD) politikaları yaygın bir uygulama haline geliyor. Bu durum işyerinde dostane ve kolay bağlantılı bir atmosferi teşvik edebilse de, aynı zamanda bir güvenlik ihlaline yol açma potansiyeli de yaratmaktadır. Kuruluşunuzun bir BYOD politikası varsa veya bir politika uygulamayı düşünüyorsanız, dolandırıcılıkları, kötü niyetli bağlantıları ve zayıf şifreleri tanımlamak için şirket çapında çalışan eğitim programları ve kursları geliştirmek, uygulamak ve uygulatmak önemlidir. Şifre gereklilikleri genellikle güvenlik açıklarından geçer.

2015 yılında yapılan bir güvenlik analizi, zayıf uzaktan erişim güvenliği ile birlikte, ihlallerin yüzde 94'ünün zayıf şifrelerden kaynaklandığını tespit etti. (Price, 2019)

Siber güvenlik, bir kuruluşun her düzeyinde çok önemlidir ve bir güvenlik bilinci kültürünün benimsenmesi BT bağlantısının başarısızlığı ile başarı arasındaki fark anlamına gelebilir. Neyse ki, siber saldırıları önleme adına atılan siber güvenlik adımları stratejik olarak kurum ve kuruluşların ellerini güçlendirerek, siber saldırılardan daha az maddi ve manevi kayıpla ayrılmalarına zemin hazırlamaktadır. İşte bu nedenledir ki siber güvenlik kavramı yaşanan zararı azaltacak en temel yapı taşıdır.

- Senaryo 17: Ulusal Elektrik Şebekesine Terör Saldırısı Senaryosu

Söz konusu saldırı senaryosunda, ulusal elektrik şebekesinin bir kısmına varsayımsal bir terörist saldırının risk değerlendirmesini sunmaktadır. Böyle bir siber saldırının getirdiği bazı sonuçlar incelenerek değerlendirmeler yapılmıştır. Amaç, birkaç büyük metropol alanına hizmet veren elektrik şebekesinin belirli bir bölgesine siber terör saldırısı riski hakkında bilgi elde etmektir. Risk yönetimi, elektrik sektörünün "kritik altyapı koruması" programının ayrılmaz bir parçasıdır. Yapılan bu senaryo sayesinde esas olarak, ulusal elektrik altyapısının temel bileşenlerinin fiziksel ve siber tehditlere karşı, hem sanayi bazında hem de sanayi-hükümet ortaklıkları ile uygun risk yönetimi sayesinde tutarlı bir şekilde korunması amaçlanmış ve bununla birlikte bölge halkının elektrik sektörüne olan güveninin korunması amaçlanmıştır. Senaryomuzda bir

elektrik şebekesine hem siber saldırı gerçekleştirilmiş hemde aynı zamanda fiziksel saldırıda gerçekleştirildiği varsayılmıştır.

Siber saldırı her alt istasyondaki ekipmana, ağa ve bölgeye değişen derecelerde hasar vererek çok sayıda fiziksel yöntem kullanılabilir. Örneğin, karbon fiberler, Mylar şeritleri veya diğer kirleticiler, ciddi kısa devrelere neden olmak için otobüsler ve transformatörler üzerine püskürtülebilir. Patlayıcılar, anahtar transformatörlerini, devre kesicileri ve veri yolu bölümlerini yok etmek için kullanılabilir. Saldırganlar ayrıca trafo merkezi işletim panellerindeki devre kesici kontrollerine de zarar verebilir. (Garrick, 2008)

Bu senaryoların modellenmesine yardımcı olmak için, bir tehdit değerlendirmesinin, elektrik şebekesi hakkında ayrıntılı bilgilerin teröristlere sunulması olasılığının yüksek olduğu varsayılmaktadır. Analiz yöntemini açıklamak için, önce trafo merkezi incelenir, çünkü üretim istasyonundan tam verimde ve siber saldırı sonrası güç kaybını görmek açısından önemlidir.

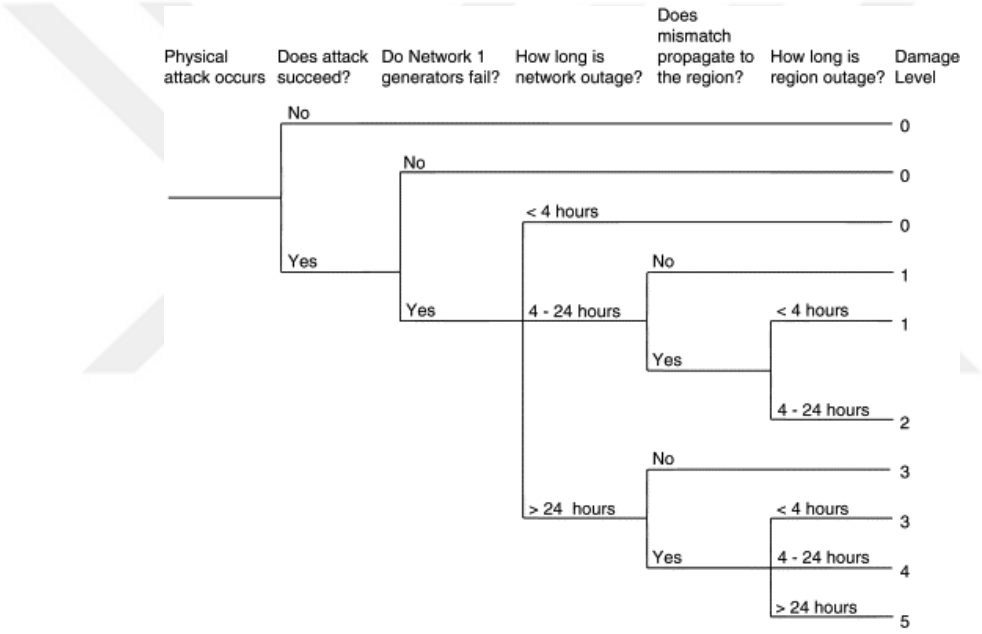
Saldırı senaryolarını oluşturmak için beş ardışık soru sorulur.

1. Saldırı başarılı mı? Başarı, trafo merkezinin fiziksel olarak saldırıya uğradığı ve tamamen devre dışı bırakıldığı anlamına gelir.
2. Diğer tüm üretim istasyonları başarısız oluyor mu? Elektrik şebekeleri tipik olarak, bir trafo merkezi tüm ağı dengesizleştirmeden hat dışına çıkabilir. Bununla birlikte, istasyonundaki tüm devrelerin arıza tarafından başlatılan bir açıklığının, otomatik yük atma ve devre izolasyonunu diğer tüm alanlarda başlatmak için voltaj ve frekansta yeterli bir düşüşe neden olabileceği düşünülebilir. Trafoda, böylece kalan tüm jeneratörler off line hale gelmelerine neden olur. Bu nedenle, modelimiz bu olasılığı hesaba katmalıdır.
3. Elektrik kesintisi ne kadar sürer? Bu, şebekeye gücü geri kazandırmak için beklenmedik durum planlarının ne kadar hızlı uygulanabileceğine bağlı olacaktır.
4. Geçici bölge boyunca yayılıyor mu? Trafoyu ya da istasyonu dengesizleştiren fiziksel bir saldırı durumunda, bölgesel koruma sinyallerinin kalan ara bağlantıları otomatik olarak açması ve geçici akımın bitişik ağlara yayılmasını

engellemesi muhtemeldir. Bununla birlikte, geçici ve uzun vadeli kesintilerin kapsamlı bir analizi için bölgesel düzeyde basamaklı hasara neden olan arızaların olasılığı dikkate alınmalıdır.

5. Bölgesel kesintinin süresi ne kadardır? Bu, sistemin kurtarılmasını sağlamak için beklenmedik durum planlarının ne kadar hızlı uygulanabileceğine bağlı olacaktır. Şebeke içinde herhangi bir noktada geçici bir kesinti varsa, bölgesel bir kesinti için maksimum sürenin de geçici olduğu (yani 24 saatten az) olduğu varsayılır.

**Şekil 22.** Saldırı Senaryoları İçin Düşünce Süreci




**Kaynak :** (GARRİCK, 2008)

Şekil 22'de, saldırı senaryolarını geliştirmek ve sonuçlarını hasar seviyelerine atamak için kullanılan sistematik düşünce sürecini göstermektedir. Her sistemdeki diğer koruyucu engelleri hesaba katarak şubeler eklenebilir. Bu çalışmanın temel amacı, güvenlik açıklarını belirlemek için kapsamlı bir çerçeve oluşturmak ve olası tüm sonuçların dengeli bir şekilde değerlendirilmesini sağlamaktır. Şekil 22 senaryo geliştirme sürecinin karmaşık arıza ve basamaklı efekt kombinasyonlarını temsil etmek için nasıl kullanılabileceğini de gösterir. Tam ölçekli bir risk değerlendirmesi, her bir alt

istasyona yapılan saldırıların ve aynı anda birden fazla alt istasyonun etkilerini inceleyecektir.

Her durumda ulusal elektrik şebekesinin trafolarına veya istasyonlarına yapılacak olan siber saldırı ya da fiziksel saldırı 24 saatten az sürede Şekil 22'de çözülmeye çalışılan bir algoritma geliştirilmiş, kesinti yaşandığı andan itibaren bölgenin etkilenmemesi için diğer trafolar ve istasyonlar aracılığıyla hizmet verilmeye çalışılmıştır. Buna rağmen siber saldırıların enerji sektöründe hayatı kısa süreli ya da uzun dönem için felç edebileceği gerçeği asla yadsınamaz. Her durumda siber güvenlik için iletim hatlarını kullanarak diğer ana hatlardan ve yan hatlardan şehir şebekelerini besleyerek siber güvenliğin sağlanamadığı durumlarda en azından saldırının maddi kaybını en az düzeyde tutmak hedeflenmiştir. Bu sayede kısa elektrik kesintisi ile çalışanlar ve siber güvenlik uzmanları üzerindeki baskıyı en aza indirecektir.

- Senaryo 18: BATMAN İli Hidroelektrik Santrali Siber Saldırı Senaryosu

Almanya'nın Noel şirketi 2003 yılında Batman Barajının Hidroelektrik Santrali'ni bitirdiğinde, 1 milyon dolar alacağı olduğunu iddia ederek bu alacağı tahsil edemediklerini belirttiler. Bununl birlikte iş bitiminde tahsil edemediği alacakları gerekçe göstererek şirketin bilgisayarlarını şifre ile kilitlediler ve kenti terk ederek Batman İli Hidrolektrik Santralini oldukça zor bir durumda bırakarak ülkemizi terk ettiler. Yapılan bu kötü niyetli siber saldırı nedeni ile santralin üç ünitesinde de enerji üretimi tamamen durmuş oldu.

Bilgisayarların şifrelenerek kilitlenmesi nedeniyle Batman Barajı'nda enerji üretimi yapılamadığını söyleyen DSİ yetkilileri, bu nedenle Batman'ın bazı ilçeleri ile Şırnak ve Cizre'ye kesintili olarak elektrik verebildiklerini belirttiler. Barajın yeniden elektrik üretimine başlaması için şifreyi çözmek üzere Türkiye Elektromekanik Sanayi uzmanları da yoğun çalışmalarını sürdürüyor. (Milliyet Gazetesi, 2003)

Bu örnek ister bireysel olsun, isterse kamu kurumları ve sanayi kuruluşları açısından olsun, SCADA, PLC ve işletim sistemleri gibi siber çevre birimlerinin yerliliğinin önemini göstermektedir.

Burada malesef çevre birimlerinin tamamında kaynak kod yazılırken %100 yerlilik sağlanmadıkça kontrolün her ne yapılırsa yapılsın tam olarak ele alınması veya elde tutulması pek mümkün görülmemektedir.

Bu örnekte anlatılan kriz ne kadar sürdü ne kadar süre zarfında çözüme kavuşturulduğu bilinmemekle beraber ilk dalga etkisi bu elektrik kesintisinin etkilediği yerleşim birimlerinde tüketilen elektrik enerjisinin parasal değeri kadardır. Sonrasında bu maliyete bu süre zarfında tüketilen elektrik enerjisi ile gerçekleştirilebilecek üretimin maliyeti eklenmeli. Ve bu girdilerin bölgesel ekonomiye etkilerinin yanı sıra diğer bölgelerle olan ticarete etkileri de ayrıca hesaba katılmalıdır. (Özkan, 2019)

- Senaryo 19: Moonlight Maze Saldırı Senaryosu

Kamuoyunca Moonlight Maze operasyonu olarak tanınan siber saldırı Mart 1998'de başladı. Yapılan bu organize siber saldırı ile ABD'nin Pentagon, NASA, ABD Enerji Bakanlığı ve üniversitelere ait yapılan tüm araştırma ve geliştirme bilgilere ait dökümanlar, askeri tesislerin gizli ve diğer harita bilgileri, askeri eylem planları ve askeri amaçlı donanım tasarımları da dahil olmak üzere birçok gizli bilgi ve belgeler çalınmıştır.

**Şekil 23.** The Sunday Tımes Gazetesi 25 Temmuz 1999 Moonlıgt Maze Siber Saldırı Haberi



THE SUNDAY TIMES · 25 JULY 1999

OPERATION MOONLIGHT MAZE

How top secret files are being hijacked to Russia

Missing secrets

America fears Russia has stolen a treasure trove of military and industrial secrets in an unprecedented electronic intelligence offensive targeting:

information about American weapons guidance systems;

naval communications codes used by nuclear submarines;

scientific and technical intelligence from research and development institutes

# Russian hackers steal US weapons secrets

by Matthew Campbell Washington

**Kaynak :** (ÖZKAN, 2019)

Şekil 23'te Londra merkezli "The Sunday Times" gazetesinin 25 Temmuz 1999 tarihli baskısının Moonlight Maze siber saldırısının haberi görülmektedir. Haberin içeriğinde Rus hackerların ABD silahlarının sırlarını ele geçirdikleri iddiası yer almaktadır.

Aslında yapılan bu siber saldırılar 1996'da ilk olarak başladı. İlk hedefler: Wright Patterson ve Kelly Hava Kuvvetleri Üssü, Ordu Araştırma Laboratuvarı, Hint Deniz Sistemleri Komutanlığı, Maryland, NASA ve Enerji laboratuvarları. 1998'in ortalarında FBI ve Savunma Bakanlığı araştırmacıları Rus ISP'lerine işaret eden adli kanıtlara sahiptiler. (GUERRERO-SAADE, RAIU, MOORE, & RID, 2018)

1999 yılında FBI'ın Moonlight Maze siber saldırısı hakkındaki kapsamlı soruşturması kamuoyuna sızdırıldı. Maalesef ki yapılan bu saldırının aktörleri hakkındaki net bilgiler, kullanılan araçlar ve işlem basamakları hakkında bugüne kadar çok fazla ayrıntı ortaya çıkartılamadı. Sonunda kod adı farklı bir isimle yer değiştirdi (siber saldırganların "Fırtına Bulutu" olarak adlandırılan geliştirilmiş izinsiz giriş seti

daha sonra "Makers Mark" ismini aldı). Kısaltılmış hali "MM" olarak yaygın olarak bu siber saldırıyı tanımlamak için kullanıldı.

Her şey ödünç alınan tek bir istismarla başladı. Karl Grindal tarafından talep edilen FOIA belgeleri, belirli bir ortak ağ geçidi arabirimi (CGI) ikili dosyasındaki bir güvenlik açığını kötüye kullanarak askeri sistemlere yönelik çoklu saldırı girişimlerini açıklamaktadır. <phf> adlı ikili dosya genellikle o sırada HTTP arka plan programı ile paketlenmişti ve bu nedenle genellikle yüzeysel web sunucularında mevcuttu. 1996'nın başlarında bir süre, <phf> 'ye karşı bir saldırı turlara başladı. (GUERRERO-SAADE, RAIU, MOORE, & RID, 2018)

Güvenlik açığından, aşağıdaki şekilde hazırlanmış bir web isteğiyle yararlanılabilir:

- http://<server>cgi-bin/phf?Qalias=%ff/bin/cat%20/etc/passwd
  (GUERRERO-SAADE, RAIU, MOORE, & RID, 2018)

Böylece sunucu bilgisayarlar, parola dosyasının içeriğini sızdırmaya hazırlandı; böylece siber saldırganların oldukça kolay bir şekilde sunucuya ftp veya telnet göndermesi ve resmi olarak tanımlı bir kullanıcı kılığına bürünmüş bir şekilde sisteme giriş yapması sağlandı. Bazı durumlarda ise bu girişimler, sadece savunmasız <phf> ikilisinin yokluğuna dayanarak başarısız bir girişim olarak kaldı. Diğer saldırı denemelerinde, bir şekilde başarılı olmayı başardılar ve yıllar sonra bile kök salması oldukça zahmetli olan siber saldırıların önündeki bütün engelleri bir bir kaldırmış oldular.

Saldırılarla ilgili yapılan iz sürme sonucunda bu saldırıların Moskova'nın 20 mil dışında yer alan ve Rusya Bilimler Akademisi ile sıkı bağları olan bir servis sağlayıcı üzerinden gerçekleştirildiği belirtilmiştir. ABD'nin milyonlarca dolar harcayarak ve yıllarca çalışarak elde ettiği deneyim, bir operasyonla el değiştirmiş oldu. Ekonomik açıdan hesaplanamayacak düzeyde bir zarar söz konusudur. (Özkan, 2019)

- Senaryo 20: Fiziksel Saldırı Senaryosu Ajan-Mikroçip

Çin casuslarının yaptığı iddia edilen sızma saldırısı, Amazon ve Apple gibi şirketlerin de içinde bulunduğu 30 büyük şirketi etkiledi. (STM Mühendislik Teknoloji Danışmanlık, 2019)

Büyük yankı uyandıran ve hükümet ve kurumsal kaynaklara göre ABD ile yapılan teknoloji tedarik ticaretini dahi riske atan bu saldırı, Bloomberg Businessweek'te "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies" çalışmasında ele alındı. 2015 yılında Amazon Portland'daki "Elemental Technologies" adlı startup kuruluşunu sessizce incelemeye başladı. (STM Mühendislik Teknoloji Danışmanlık, 2019)

Bugün "Amazon Prime Video" olarak bilinen çevrimiçi video yayın hizmetinin bu boyutlarda gelişim göstermesinde büyük payı olan bu kuruluş büyük boyutlu video dosyalarını sıkıştırma ve farklı cihazlarda çalışabilmesi için formatlama yazılımları geliştiriyordu.

Geliştirdikleri bu yazılım sayesinde, Olimpiyat Oyunlarının çevrimiçi ortamda yayınlanmasına, Uluslararası Uzay İstasyonu ile karşılıklı olarak iletişim kurulmasına ve drone görüntülerinin anlık olarak CIA'e gönderilmesinde aktif olarak rol almıştı.

Amazon Web Services'in (AWS) CIA için geliştirdiği yüksek güvenlikli bulut teknolojisinde, bu yazılımın kullanılabileceği düşünüldü. Bunun için AWS, Elemental'in güvenli olup olmadığını incelemek adına üçüncü bir şirketle anlaştığını duyurdu. İlk bulgulara göre AWS'den, Elemental'in ana ürününün daha sıkı incelenmesi istendiği bildirildi. Kaynaklara göre, Elemental'in kullandığı ve müşterilerin video sıkıştırmak için ağlarına kurdukları bu pahalı sunucular, dünyanın en büyük sunucu anakart tedarikçilerinden biri olan San Jose merkezli Super Jose Computer Inc. şirketi tarafından geliştiriliyordu. 2015 baharında, Elemental firmasından birkaç sunucu incelenmesi için bahsi geçen güvenlik şirketine gönderildi. (STM Mühendislik Teknoloji Danışmanlık, 2019)

Bu güvenlik şirketi ayrıntılı olarak yapılan incelemelerde sonucunda sunucu anakartlarına entegre edilmiş halde pirinç tanesinden daha küçük boyutlarda Şekil 24'te gösterilen bir mikroçipi tespit ettiğini açıkladı.

**Şekil 24.** Sunucu Anakartlara Yerleştirilen Anakart




**Kaynak :** (STM MÜHENDİSLİK TEKNOLOJİ DANIŞMANLIK, 2019)

Amazon bu durumu yetkili ABD makamlarına bildirdi. Elemental'in sunucuları, Savunma Bakanlığı veri merkezlerinde, CIA'in drone operasyonları biriminde ve Donanma savaş gemilerinin ağlarında kullanılıyordu ve Elemental, yüzlerce mikroçip müşterisinden yalnızca biriydi. (STM Mühendislik Teknoloji Danışmanlık, 2019)

Üç yıldan daha uzun süren gizli bir soruşturma sonucunda raportörler, bu mikroçiplerin saldırganlara istemli olarak ağa sızabilmeleri için gizli bir açık kapı bıraktığını belirttiler. Araştırmacılar ayrıca bu mikroçiplerin Çin'de taşeronlar tarafından işletilen fabrikalara yerleştirildiğini tespit etmişlerdi. Bu, insanların genelde karşılaştığı yazılım tabanlı tek düze tipte saldırılardan çok daha farklı bir saldırı olarak gün yüzüne çıkartılmıştı. Ayrıca uzmanlara göre, donanımsal saldırılar potansiyel olarak yazılımsal saldırılara göre çok daha yıkıcı etkiye sahiptiler ve bunları tespit edip önlem almak kurumlar için oldukça zor ve karmaşık bir yapıya sahipti.

2015 Eylül ayına gelindiğinde ise Amazon, Elemental'i satın aldığını duyurdu. Amazon, Apple ve Supermicro, Bloomberg Businessweek'in konuyla ilgili raporlarını inceleyerek siber güvenlik adına alınabilecek önlemleri masaya yatırdılar.

Amazon, "AWS'nin tedarik zincirinde herhangi bir taviz verilmemiştir. AWS'nin kötü niyetli çipler veya Elemental'ı satın alırken anakartlardaki donanım değişiklikleri hakkında bilgisi yoktu" şeklinde bir açıklama yaptı. Apple tarafından ise, "Bu konuda oldukça açık olabiliriz: Apple herhangi bir sunucuda kötü niyetli çip, donanım manipülasyonları veya güvenlik açıkları bulmuş değildir" açıklaması geldi. (STM Mühendislik Teknoloji Danışmanlık, 2019)

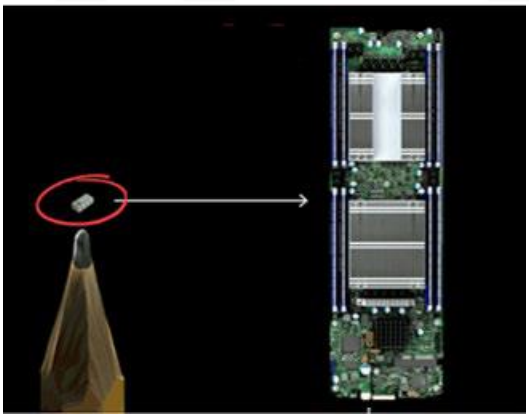
Supermicro şirketinin yaptığı açıklamaya göre yapılan bir soruşturmadan bilgilerinin olmadığını belirttiler. Çin hükümeti ise, Supermicro sunucularının manipülasyonuyla ilgili doğrudan açıklama yapmak istemedi ve bunun yerine "Siber güvenlik alanında tedarik zinciri güvenliği ortak bir sorun ve Çin'de bir kurbandır" şeklinde bir açıklama yayınladı. CIA ve NSA'yi temsilen ise konuyla ilgili yorum yapmaktan kaçınıldı.

ABD resmi kaynaklarından konuya bakıldığında ise, Çin'in ilgili askeri birimi bir kalem ucundan çok daha küçük boyutta bir mikroçip tasarlayıp imal etmişti. Tasarlanan bu mikroçipler siber saldırı düzenleyebilmek için gereken hafıza, ağ yeteneği ve yeter seviyede işlemci hızına sahip şekilde üretilmişlerdi.

Bu mikroçiplerin dünyanın önde gelen sunucu anakart satıcılarından biri olan Supermicro'nun tedarikçileri olan Çin fabrikalarına yerleştirildiği tespit edilmişti. (STM Mühendislik Teknoloji Danışmanlık, 2019)

Ele geçirilmiş olan bu anakartlar (Şekil 25) Supermicro'nun sunucularına yerleştirilmişti.

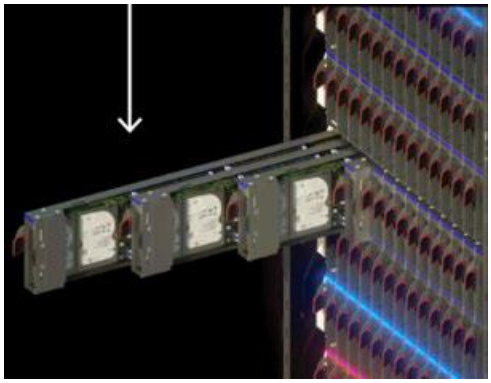
**Şekil 25.** Zararlı Mikroçipin Entegre Edildiği Sunucu Anakartı



**Kaynak :** (STM MÜHENDİSLİK TEKNOLOJİ DANIŞMANLIK, 2019)

Zararlı hale gelmiş olan bu anakartların bağlı olduğu sunucular da Şekil 26 gösterilen haliyle zararlı sunucu haline gelmişlerdi ve bu sunucular düzinelerce şirket tarafından işletilen veri merkezlerinde bulunuyordu.

**Şekil 26.** Zararlı Hale Gelmiş Anakartın Bulunduğu Sunucu



**Kaynak** : (STM MÜHENDİSLİK TEKNOLOJİ DANIŞMANLIK, 2019)

Uzmanların açıkladığı bilgilere göre, bir sunucunun açılışı sırasında bu zararlı mikroçip sunucunun işletim sisteminin çekirdeğini değiştirmek kaydıyla işletim sistemini modifikasyonlara açık hale getiriyordu bu sayede saldırıya zemin hazırlanmış oluyordu. Mikroçip aynı zamanda siber saldırganlar tarafından kontrol edilen bilgisayarlarla iletişime geçebiliyor ve istenmeye komut dizelerini çalıştırıp kodlamaya açık hale getiriyordu.

McLean'daki brifingden sonra geçen üç yılın ardından, Supermicro'nun anakartlarındaki saldırıları tespit etmek için ticari olarak uygun ürün çıkmadığı ve çıkmasının da muhtemel olmadığı bildirildi. Apple ve Amazon'un kaynakları böyle bir saldırının tespitinin yapılmış olmasının bile şans eseri olduğunu ifade etti. Bu saldırının uç nokta bir saldırı olduğu ve kolay kolay teknolojik bir çözüm getirilemeyeceği belirtildi. (STM Mühendislik Teknoloji Danışmanlık, 2019)

- Senaryo 21: ABD Sağlık Sigortası Sistemine Düzenlenen Sanal Siber Saldırı

ABD sağlık sistemine yapılan sanal siber saldırı sonucunda elde edilen bilgiler sayesinde sistem oldukça büyük maddi kayıplara uğramış. Yapılan saldırıyı önleyebilmek adına hasta kayıt ve bilgilerinin tutulduğu sistem bir süre geçici olarak kapatılmıştır. Siber saldırılar konusunda oluşturulan karşı ekip sorunun kaynağını çözmeye çalışmış, bu süreçte maddi ve sistemin itibar ve güvenilirlik açısından manevi kayıpları söz konusu olmuştur.

Senaryoya göre hasta kayıt sistemine sızılarak yapılan saldırı sonucunda izinsiz kopyalanan hasta kayıtları, şifre bilgileri, adres defteri bilgileri, kimlik bilgileri, reçete

edilen ilaç bilgileri vs gibi bilgileri derin webte satmak istenmiştir. Sağlık sistemin bir müşterisi olan kişinin tesadüf eseri derin webte gezerken kendi üyesi olduğu sistemin hasta kayıtlarının satılık olduğunu görünce ihbarda bulunmuş daha sonra sistemin güvenlik uzmanları tarafından gerekli araştırma ve müdahale yapılmış, sisteme etkileri uzmanlarca analiz edilmiştir.

Aslında bir siber saldırının bir kuruluşu etkilemesinin birçok yolu vardır ve bu etkiler, ürünün niteliğine ve ciddiyetine bağlı olarak değişecektir. Yapılan bu siber saldırının etkilerinden bazıları iyi bilinen doğrudan maliyetlerdir. ABD sağlık sistemine düzenlenen bu siber saldırıda maddi kayıplar, borsadaki değer kayıpları, kredi notunun düşmesi gib ciddi boyutlara ulaşmıştır. Fakat ABD sağlık sisteminin esas kaybı diğer kayıplar olarak adlandırabileceğimiz manevi kısmı olan daha geniş kapsamlı, maddi olmayan maliyetlerdir nicelleştirilmesi daha zor olan kayıplar diyebiliriz. Bu aşamada yapılan bu siber saldırının sonucu olarak hastalar ve sisteme üye olan kişilerin bilgilerinin kopyalanması ile sisteme olan güven kaybı, yeni hasta kayıt oranının güven bunalımı nedeniyle düşmesi, sistemin halkın gözünde uğradığı itibar kaybı senaryo dahilinde değerlendirilmiştir.

Saldırı senaryosunun yapıldığı ABD sağlık sistemi şirketinin aşağıdaki yapıda olduğu senaryoya göre varsayılmıştır.

**Tablo 1** Sanal Abd Sağlık Sistemi Kuruluşu Yapısı

| Sanal ABD Sağlık Sigorta Sistemi Kuruluşu Hakkında |
|---|
| 60 milyar dolarlık yıllık gelir |
| 50.000 çalışan |
| ABD genelinde 23,5 milyon üye (yüzde 60'ı işveren sözleşmeleri yoluyla abone oldu) |
| Tıbbi uyarılar sağlayan ve sağlayıcı ağındaki sağlık pratisyenlerinin hasta kayıtlarına ve sigorta kapsamı bilgilerine erişmesine izin veren bir hasta bakımı uygulaması kullanır |
| Kasım-Ocak ayları arasında açık kayıt yaptırır (insanların sağlık sigortası planlarına |

| |
|---|
| kaydolabileceği yıllık dönem) |
| Hem devlet hem de federal yetkililer tarafından düzenlenmiştir |
| Bir sağlık sistemi elde etmek için borç sermayesinde 1 milyar dolar toplamayı planlıyor |
| 100 milyon dolarlık siber sigorta poliçesi için yıllık 7 milyon dolar prim öder |

**Kaynak** : (DELOITTE DANIŞMANLIK ŞİRKETİ, 2016)

Yapılan bu siber saldırı senaryosunun gelişimi ve ayrıntılı sonuçları aşağıda belirtilmiştir.

Mayıs ayında şirket, 2.8 milyon kişisel sağlık bilgisi (PHI) kaydı içeren bir dizüstü bilgisayarın, şirketin sağlık analizi yazılım satıcısından çalındığını öğrendi. Bu uzlaşma, beş gün sonra şirkete kurumsal bir müşteri tarafından müşterinin çalışanlarından bazılarıyla ilişkili bilgilerin siber suç "karanlık web" sitelerinde satışa sunulduğunu bildirdiğinde ortaya çıktı. Aynı zamanda, hasta bakımı uygulamasının yöneticileri, oluşturulan yeni kullanıcı hesabı sayısında ve aktif kullanımda önemli bir artış fark etmeye başladı. Ayrıca, bir milyon ek hasta kaydının uygulama veritabanından indirildiğini ve yetkili kullanım için olduğunu doğrulayamadığını tespit ettiler. Sonuç olarak, şirket hekimin hasta bakımı uygulamasına erişimini kapattı ve siber olay müdahale ekibini etkinleştirdi. Olay araştırılırken başvuru iki hafta boyunca çevrimdışı tutuldu. Bu süre zarfında, şirket ile hekimleri ve sağlayıcıları arasında kapsama ve hak taleplerinin validasyonu, şirketin çağrı merkezinde "aşırı destek" sağlamak için profesyonel bir hizmet kuruluşundan hizmet alınarak yapıldı. Teknik araştırma, siber saldırganların çalınan dizüstü bilgisayardan ayrıcalıklı kimlik bilgileri kullanarak hasta bakımı uygulamasına eriştiğini ve önemli sayıda kullanıcı kimliği oluşturduğunu ortaya koydu. Sonuç olarak, hizmet geri yüklenmeden önce, tüm uygulama kullanıcıları için yeni kullanıcı hesapları yayınlanmalı ve yeni uygulama ile sistem kontrollerini yaparak veriler tekrar erişime açılmalıdır. (DELOITTE Danışmanlık Şirketi, 2016)

Bu siber saldırının toplam maliyeti beş yıllık bir zaman dilimi içinde 1,6 milyar dolardan fazlaydı ve önemli bir ilgi gördü, etkinin sadece yüzde 3,5'i "yüzeyin üstünde" idi. Sıradan gözlemciye göre, bu olay PHI veri hırsızlığının klasik bir örneğiydi ve

şirket müşteri bildirimi, müşteri koruması ve düzenleyici para cezaları da dahil olmak üzere bir veri ihlali konusunda ortak sonuçlar doğururken, çok daha derin etkileri vardı. Gerçekte, etkinin yüzde 96'sından fazlası "yüzeyin altında" idi. Dahası, etkinin neredeyse yüzde 89'u sadece 3 "yüzeyin altında" etki faktörüyle ilişkiliydi: kaybedilen sözleşme gelirinin değeri; ticari adın devalüasyonu; ve müşteri ilişkilerinin değer kaybı. (DELOITTE Danışmanlık Şirketi, 2016)

Bir başka ilginç gözlem, etkinin zamanla nasıl oynandığıdır. Triyaj aşamasındaki "kanamayı durdurma" maliyetlerinin toplamı, toplam finansal etkinin yüzde 4'ünden daha azını oluşturdu. Etki yönetimi aşamasındaki etki yaklaşık yüzde 40'a yükseldi. Ancak bu, olaydan sonraki yıllarda gerçekleşen etkinin yaklaşık yüzde 57'sinin, bir olaydan sonraki yılın en etkili olduğunu düşünerek zorlandığı anlamına geliyordu. Bu senaryoda, en büyük etkiler zamanla ortaya çıkan daha az belirgin faktörlerdir. Aşağıda, en etkili üç faktörün nasıl tahmin edildiğine dair bir açıklama bulunmaktadır. (DELOITTE Danışmanlık Şirketi, 2016)

Kayıp sözleşme gelirinin değeri (primler): Bu senaryoda sözleşmeler iptal edilmedi, ancak şirket olayın zararını azaltmaya çalıştığından, üyelerini tarihsel olarak tahsil ettikleri prim artışını ayarladı. Bu, beş yıl boyunca tahmini 830 milyon dolar zararla sonuçlandı. Bu hesaplamaya ulaşmak için, yıllık primlerdeki ortalama artışın birinci yılda yüzde 20 oranında azaldığı ve prim büyüme oranlarının, beş yıl sonra olayın öncesine kıyasla ortalama büyüme oranlarını karşılamak için istikrarlı bir şekilde arttığı varsayılmıştır. (DELOITTE Danışmanlık Şirketi, 2016)

Ayrıca, bu hesaplama, birinci yılda yeni üyelerin (ihlalden hemen sonra) yüzde 50 azaldığı varsayılmıştır. Bununla birlikte, yeni üyeler için büyüme oranı sürekli olarak normal büyüme oranlarına yükseldi, böylece dördüncü ve beşinci yıllarda sırasıyla yüzde 25 ve yüzde 30 büyüme oranlarına ulaşıldı. Siber saldırıdan önce, şirketin müşteri ilişkilerinin veya üyelerinin toplam değerinin 10.3 milyar dolar olduğu tahmin ediliyordu. Beş yıllık dönemde modellenen kayıp üyeler veya müşteriler nedeniyle yıllık gelirlerdeki düşüşe bağlı olarak, müşteri ilişkilerinin değeri 9,5 milyar dolara geriledi. Bu kayıp, yukarıda atıfta bulunulan kayıp sözleşme gelirine (primler) ek olmuştur. (DELOITTE Danışmanlık Şirketi, 2016)

- Senaryo 22: Şifre İçeren Şifreli Dosyayı Çözme

Öncelikle güçlü şifre güvenliğine değinmekte fayda var. Çağımız teknoloji dünyasında kullanılan tüm cihazların güvenliğinin sağlanması açısından şifre kullanılır, fakat kullanıcıların internet ortamında güvenliğini sağlaması için belirledikleri şifreler çoğunlukla hılı giriş yapmaya yönelik akılda kalıcı, basit ve aynı olmaktadır. İnternetin bir çok ortamında aynı şifrenin veya benzerlerinin kullanılması tahmin edilebilir bir güvenlik açıklığı yaratmaktadır. Şifre kullanımı önemlidir fakat güçlü şifre kullanımı daha önemlidir. Güçlü şifre ad, soyad, doğum tarihi, evlilik tarihi, telefon numarası veya memleket gibi, ardışık sayılar veya harfler, kişisel bilgi ile oluşturulan basit ve tahmin edilebilir olmamalıdır. Güçlü parola; tahmin edilmesi zor, büyük küçük harf, rakam ve özel karakterler içermelidir.

Günümüzde bu şifreleme yöntemlerine dikkat edilse de bazı durumlarda şifre güvenliğinde iki faktörlü kimlik doğrulaması teknolojilerinden de yararlanılması gerekmektedir.

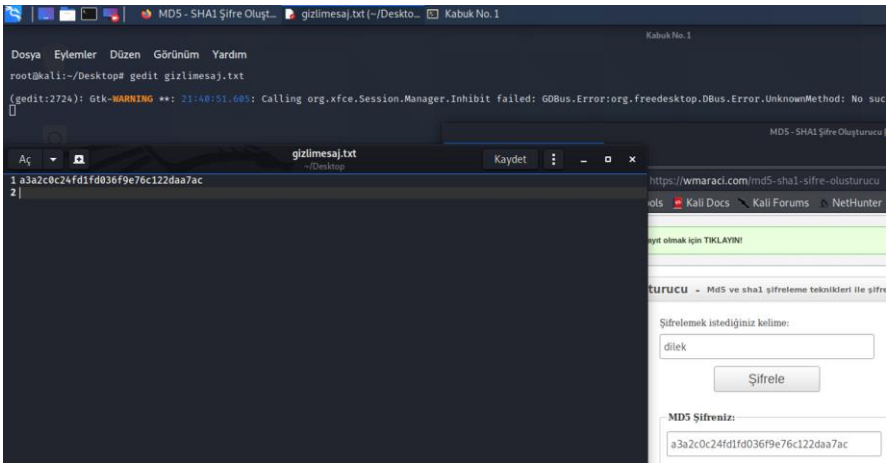
Güvenlik şirketlerince yapılmış olan araştırmalar neticesinde dünya genelinde en çok 123456 şifresinin kullanıldığı tespit edilmiştir. Türkiye'de ise en fazla kullanılan şifreler aşağıda yer almaktadır.

123987456 / q1w2e3r4 / istanbul24 / 06ankara / password / parola / sanane / bjk1903 / 19921992 / 123456789 / cimbom / fenerbahce / 112233

Örnek olarak gizli bir şifreli mesajın barındığı şifreli bir dosyaya erişimimiz mevcut. Bu dosyaya erişilmesi ardından içerisindeki şifreli metnin çözülmesini istiyoruz. Sızma testlerinde kullanılan Hashcat yöntemi ile bu işlem yapılabiliyoruz.

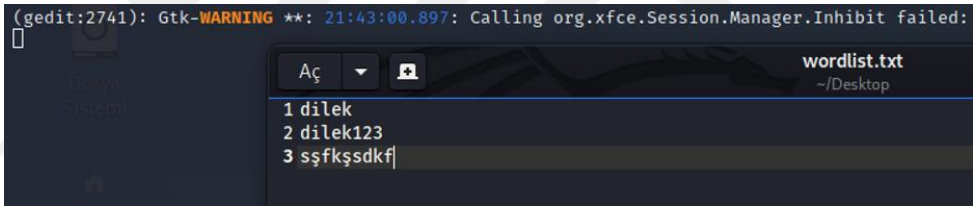
Hashcat, basitçe hash kırma işlemlerini otomatize yapmak için kullanılan bir araçtır. Hash kırma işleminde en basit yollardan biri olan parolayı tahmin edip hashini alıp karşılaştırma yapmak yöntemlerden biridir. Dictionary ve brute-force saldırıları parolaları tahmin etmenin en yaygın yollarıdır. Brute-force çalışma mantığı çok karmaşık olmayıp verilen aralığa göre tüm kombinasyonları deneme şeklinde gerçekleştirilir. Buda demek oluyor ki brute-force için oldukça zaman gerekir. Dictionary saldırısında ise wordlist ile doğru orantılıdır. Ben deneme işlemimde Dictionary saldırısı üzerinden ilerledim. (ŞAN H. )

**Şekil 27.** Özel Metnin Şifrelenmesi Ve Kopyalanması



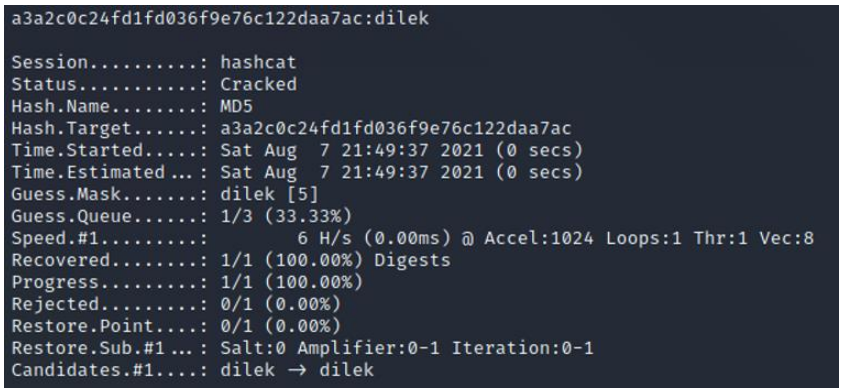

Şekil 27 de; şifrelenecek metin herhangi bir web MD5 şifreleme tekniği ile şifrelenmiş ve gizlimesaj.txt adlı dosyaya kaydedilmiştir.

**Şekil 28.** DICTIONARY SALDIRISI BAZINDA WORDLIST OLUŞTURMA




Şekil 28'de Dictionary saldırısında kullanılmak üzere bir wordlist yani adeta bir veri tabanı oluşturuldu. Bu listenin oluşturulması öncesinde elbetteki analiz çalışmaları gerekmektedir.

**Şekil 29.** Dıctıonary Saldırısı Sonucu



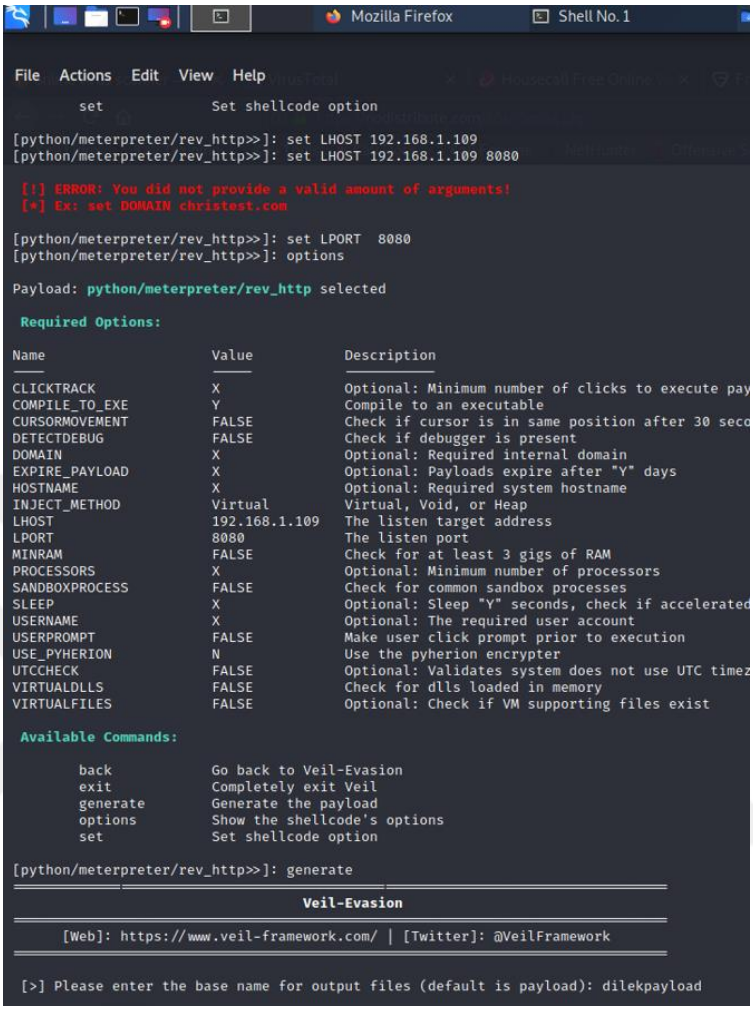

Şekil 29'da görüldüğü üzere saldırı sonucunda şifreli metnin şifreleme tekniği, hash'i, kaç denemede bulduğu ve şifre görülmektedir.

- Senaryo 23: Veil Framework'ü ile Yapılmış Zararlı Tespiti

Özellikle günümüz kurumsal hayatlarda mail yolu ile dosya veya resimlerde trojan içerikli çok sayıda zararlı bulunmaktadır. Kullanıcılar iletilen dokümanların zararlı olup olmadığını çoğunlukla anlayamadığı için kişisel cihazları üzerinde açarlar ve zararlı yerleşmiş olur. Bu sebeple bu probleme ilişkin bir örnek üzerinden ilerlenecektir.

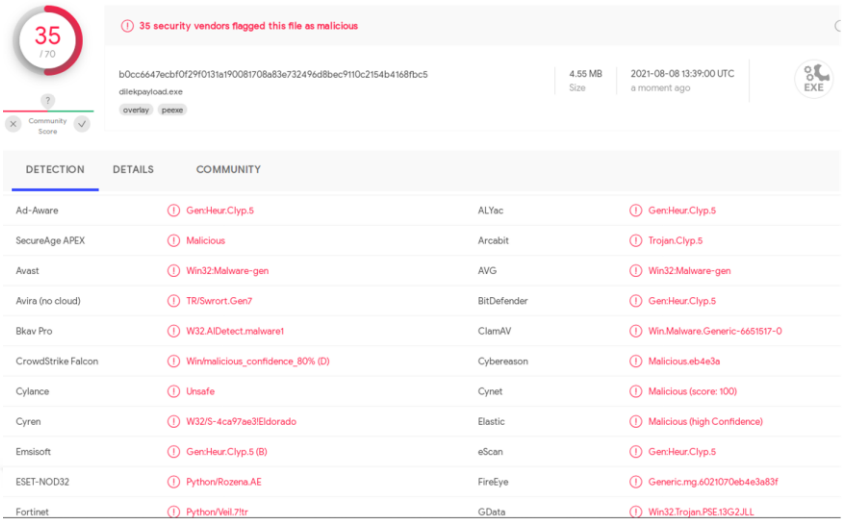
Bu işlemi yapmak için Veil Framework'ü kullanıldı. Bu framework; zararlı kodları şifrelemeye yarayan bir yapıdır. Bu sayede antivirus gibi yazılımların atlatılması sağlanır.

**Şekil 30.** Zararlı Oluşturulması




Şekil 30'da görüldüğü üzere set LHOST ile zararlının bulaştığı cihazların dinleneceği cihaz ip ve port bilgisi konfigüre edilmiştir.

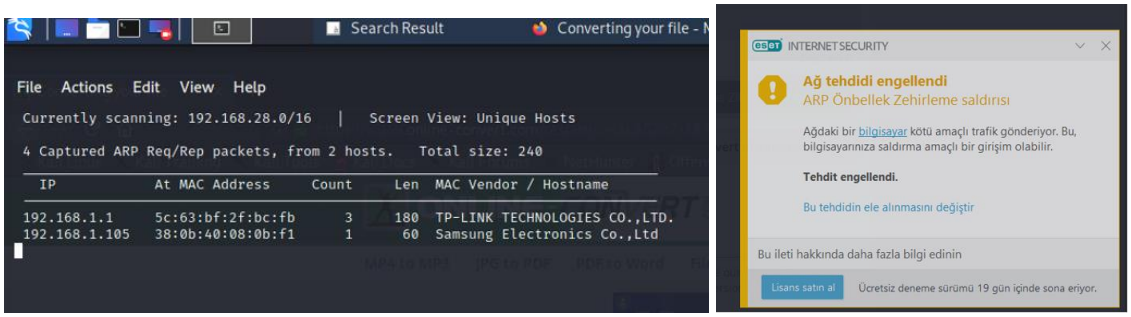
**Şekil 31.** Vırustotal Testi




Yukarıdaki Şekil 31'de görüldüğü üzere dilekpayload.exe adında oluşturulan zararlı yazılım virustotal'de bir çok güvenlik araçlarından sınıfta kalmış görünmektedir.

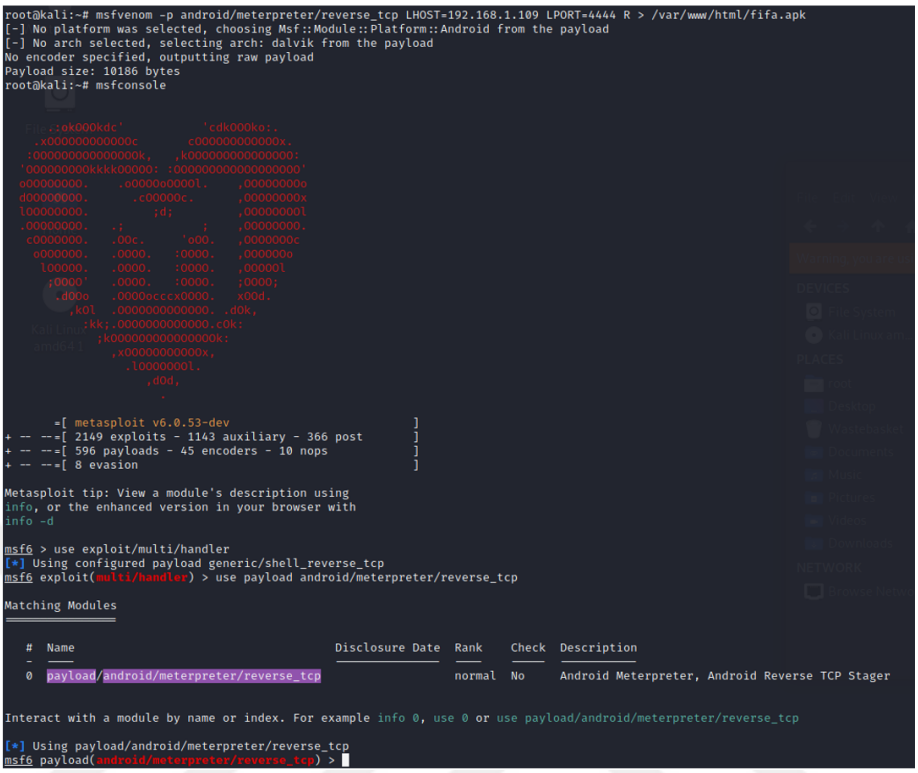
- Senaryo 24: Aynı Ağ Üzerindeki Cihaza Sızma

**Şekil 32.** Ağa Bağlı Cihazların Taranması Ve Wındows Eset Internet Securıty'e Takılması




Şekil 32'de görüldüğü üzere Kali Linux üzerinde aynı ağa bağlı cihazların taraması yapılarak IP, Mac adres ve Marka bilgileri elde edinilmiştir. Ayrıca Kali Linux'un bulunduğu fiziksel bilgisayarın da aynı ağda bulunmasından dolayı bilgisayarda yüklü antivirus sayesinde bu taramanın Windows bilgisayarda engellendiği görülmüştür.

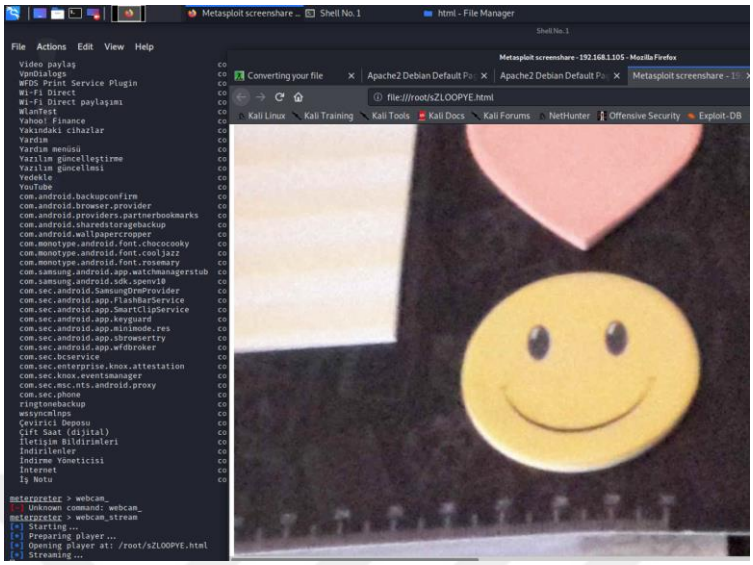
**Şekil 33.** Sızma Konfigürasyonları

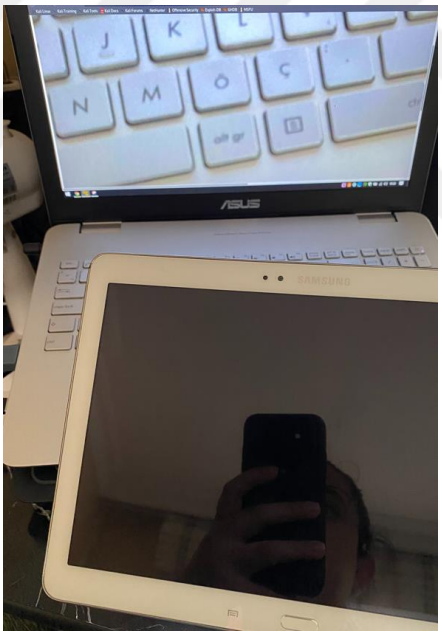



Şekil 33'de; msfvenom tool'u ile android cihazımıza sızmak için gerekli konfigürasyonları yapıldı. Dinlenecek port(LPORT-Kali) ve ip(LHOST-Kali) bilgisi yazıldı, ayrıca exploit sisteminde hangi payload kullanılacağı bilgisi eklendi. Karşı tarafı kandırmak amaçlı fifa.apk adında bir ajan oluşturuldu ve bu oyun gibi sergilendi.

İlgili (sözde) oyunun LHOST diye belirtilen Kali'nin adresi/fifa.apk şeklinde android cihazda browser'da yazıldı ve uygulama indirildi. Android cihaz üzerinde çalıştırıldıktan sonra Kali üzerinden artık bu cihaza sınırsız erişim verilmiş oldu.

**Şekil 34.** Androıd Cihazda Arka Kameradan Görüntü Alınması




Şekil 34 ve 35'de görüldüğü üzere fifa.apk adlı yalancı oyunun indirilip çalıştırılmasından sonra Şekil 34'de görülebileceği gibi webcam_stream komutu kullanılarak Android cihaz üzerinde arka kamerasına erişilmiş ve canlı olarak Kali üzerinde görüntülenmiş oldu. Bu gibi durumlarda kameranın olduğu bölgenin ısınması kullanıcılar için bir uyarı teşkil edebilir. Ayrıca android cihazların ayarlarında bilinmeyen yayıncılardan uygulama indirilmemesi için gerekli ayarlar da bulunmaktadır.

Ana hatlarıyla ortaya konulan senaryolar farklı endüstrileri ve saldırı hedeflerini temsil eder ve bir siber saldırının ortaya çıkmasının birçok yolunu gösterir. Her ne kadar bu çaba için basitleştirilmiş olsa da, senaryolar tanımlanmış etki faktörlerinin şirket, olay ve yanıta dayalı olarak oynadığı benzersiz yolları gösterir. Özetle, örnekler bir siber saldırının tipik olarak düşünülenden daha geniş bir iş etkileri kümesi içerebileceğini ve bu etkilere değinmenin çok karmaşık olabileceğini ve bazı durumlarda "yüzeyin üzerindeki" siber saldırı etkilerinden daha maliyetli olabileceğini vurgulamaktadır.

Veri ihlallerinde yaygın olarak görülen "yüzeyin üstünde" maliyetleri buzdağının sadece görünen kısmı olabilir ve genel etkilere kıyasla nispeten küçüktür.

Senaryomuzda, tipik veri hırsızlığı içeren bir saldırıda bile, veri ihlali yanıtıyla ilişkili klasik "yüzey üstü" maliyetlerinin olay boyunca en belirgin olamayabileceğini göstermektedir.

Bir siber saldırının etkisi, bir olayı takip eden yıllar boyunca ortaya çıkar.

Acil triyaj aşaması maliyetlidir, ancak uzun vadeli çabalar çok daha büyük bir ücret alabilir. Davetsiz misafirlerin çıkarılmasından ve kamuoyu incelemesinin azalmasından çok sonra, bir siber saldırının etkileri çok yıllı bir zaman çizelgesinde yankılanabilir. Çalınan veriler zaman içinde çeşitli şekillerde kullanıldığından yasal maliyetler artabilir; olay öncesi büyüme ve kârlılık seviyelerinin geri kazanılması yıllar alabilir; ve marka etkisi çeşitli şekillerde ortaya çıkabilir.

Bir saldırıdan kurtulmak sadece teknik bir çaba değildir.

Her ne kadar siber saldırılar teknoloji tabanlı araçlarla yapılsa ve altyapı, ekipman ve uygulamalarda çok önemli hasara yol açabilse de, büyük hasar genellikle BT varlıklarının kendilerine değil, işletme değerine olacaktır. Olay yanıtı öncelikle teknik bir çaba değildir. Senaryoların gösterdiği gibi, bilgisayar sistemlerini araştırmak, analiz etmek, temizlemek ve onarmak için teknik çalışma kısa sürede önemli iş liderliği olan müşteri ve üçüncü taraf ilişkilerini, yasal konuları, yatırım kararlarını ve stratejik kursta yapılan değişiklikleri yönetme çabalarıyla gölgede bırakılacaktır.

# BÖLÜM 4. SONUÇ VE DEĞERLENDİRME

Bu çalışmada siber güvenliği sağlama açısından dünyada ve ülkemizde yaşanan siber saldırılar ve sanal siber saldırı senaryoları incelenmiş ve oluşturulmuştur. Bununla birlikte incelemenin sonucunda maddi ve manevi kayıpların boyutları ele alınmış olup, bu tarz bir saldırının kötü sonuçlar doğurmadan engellenmesi amacıyla alınabilecek siber güvenlik önlemleri hakkında ayrıntılı değerlendirmeler yapılmıştır.

Yaşanılan teknolojik gelişmeler çağımızda baş döndürücü bir hızla insan hayatına değişimler getirmektedir. Bu değişimler insan hayatını olumlu etkileyebildiği gibi olumsuz sonuçlarda doğurabilir. Örneğin tez çalışmamızda bahsettiğimiz gibi Estonya devletinin teknolojik çağa ayak uydurması baş döndürücü bir hızla gerçekleşmiştir, öyle ki bir kaç yıl içerisinde toplumun çok büyük bir kısmı devlet işlemlerini, bankacılık işlemlerini, alış veriş işlemlerini ve daha birçok işlemi sanal dünyada tek tıkla yapabilir hale gelmiştir. Fakat bu başdöndürücü gelişmeler olurken acaba "siber güvenlik" kavramını önemsediler mi? Bunun cevabını malesef ülkedeki başbakanlık resmi internet sitesi, kamu kurum ve kuruluşları, özel şirketlere sistematik ve anlık olarak yurt dışından yapılan ani ve başarılı olan siber saldırı atağı karşısında "siber güvenlik" kavramı için gerekenleri tam anlamıyla yapmamalarının faturasını fazlasıyla ödediler. Sadece bununla kalındığını düşünmek ise hayalperestlik olurdu, bu saldırının sadece görünen ve tespit edilebilen yüzüydü. Devamında kaç sisteme sızdıklarını tespit edebilmek neredeyse imkansızdı. Çünkü ağları siber güvenlik yazılımları ile desteklenmediği için log kayıtları ve siber saldırganların arkada bıraktıkları izleri toparlamak oldukça zor bir işlem haline geldi.

İşte bu sebepledir ki siber saldırıya uğramadan siber güvenlik kavramı için çalışan yazılımları ve siber güvenlik uzmanlarını aktif, çalışır ve güncel vaziyette tutmanın önemi tüm dünyada devlet bazlı bir krizle yani Estonya siber saldırısı ile ortaya çıkmıştır.

Yaşanan bu siber saldırıların sonucunda artık kişisel kullanıcıların bile hedef olduğu sonucu kendini göstermiştir. Bu sebeple ortaya çıkan siber güvenlik kavramı

yaşanan saldırıların yoğunluğu arttıkça kurumların ya da şahısların yeniden olayları tüm boyutlarıyla değerlendirmeleri gerektiğini ortaya koymuştur.

Çeşitli ülkelere mensup üyeler barındırabilen siber saldırganlar internet sayesinde kolayca organize olabilmekte ve düzenledikleri siber saldırılarla ülkelere, şirketlere, kamu ve tüzel kişiliklere azımsanamayacak ölçüde büyük zararlar verebilmektedir. İşte tüm bbu yaşanan saldırıları, maddi ve manevi boyutlarını değerlendirecek olursak, karşımıza tek bir sonuç çıkmatadır, o da: "Siber güvenlik kavramı tam olarak sağlanamadığında çevrimiçi ya da intranet ortamında siz ve verileriniz asla güvende değilsiniz." gerçeğidir.

Yaşanan siber saldırılardan yola çıkacak olursak ciddi maddi ve manevi zarara uğramak istemiyor ve hizmetleriniz aksamadan devam etsin istiyorsak bir nevi iş güvenliği önlemi sağlamak gibi düşüneceğimiz "siber güvenlik" kavramına ve bunun gereklilikleri olan özelliklere mutlaka ama mutlaka dikkat etmemiz gerektiğidir. Siber güvenlik için, parolalarınız güçlü parolalar olmalı, gereksiz kullanıcı yetkilendirmeleri yapılmamalıdır. Örneğin bilgileri sadece okuması gereken kullanıcıya yazma - düzenleme - silme gibi bütün yetkilerle donatım yapmamıza gerek yoktur. Bununla birlikte mutlaka siber yazılımlarınız güncel tutulmalı, antivirüs ve casus yazılım izleme programları mutlaka kullanılmalı, şifreyi ve kullanıcı adını otomatik olarak kaydet seçeneği asla kullanılmamalı, bilgisayarınızın başından kilit ekranı açılmadan kalkmamanız önerilmektedir. Kişisel bilgi, şifre ve belgelerinizi güvenseniz dahi kimseyle paylaşmamalısınız. Siber güvenlik kurallarına uyum sağlamak adına yapılacakları kaçırmak veya kayıtsız kalmak kuruluşların ve kişisel kullanıcıların beklemedikleri ciddi boyutlardaki zararlara uğramalarına neden olmaktadır.

Değerlendirmemizi yaparken ABD'nin enerji sektörüne düzenlenen sanal saldırı senaryosuyla karşılaştığı saldırı senaryolarına göre minimum zararı ülke ekonomisinine 21 milyar dolar olarak belirlenmiş, en uç senaryoda ise toplam zararın ülke ekonomisine 1 trilyon doları aşan bir rakama ulaşması değerlendirilmiştir. İşte bu senaryoya göre elde edilen değerlendirme sonucu oluşan büyük zarar bile aslında siber güvelik kavramının siber saldırılarda önleyici olarak kullanılması gerekliliğini ortaya koymuştur, eğer ki oluşacak tüm zarara katlanmak istemiyorsanız tabi ki.

Çalışmamızda yayınladığımız tüm gerçek ve sanal saldırı senaryolarının oluşturduğu veya oluşturabileceği sonuçlar aslında çağımızda siber güvenlik kurallarına uymanın gerekliliğini ortaya koymuştur. Şirtketiniz, kuruluşunuz ve kendiniz için ya bilinen siber güvenlik kurallarına uyun ya da profesyonel siber güvenlik uzmanlarından mutlaka profesyonel düzeyde yardım alın ki senaryolarda belirtilen büyük maddi ve manevi zararlar sizinde yaşanmış gerçeğiniz olmasın.

Sonuç olarak artık kurumlar siber güvenlik yazılımlarını saldırıya uğramadan değil, saldırı öncesinde hazır ve güncel halde tutmalılar ki itibar kaybı ve maddi kayıplar yaşamadan bu tehlikeyi atlatabilsinler.

# KAYNAKÇA


Başakçı, G. (2019, Mayıs 27). *Siber Güvenlik Saldırılarının Motivasyon ve Amaçları*. BGA Security: https://www.bgasecurity.com/2019/05/siber-guvenlik-saldirilarinin-motivasyon-ve-amaclari-bolum-5/ adresinden alınmıştır

Deloıtte Danışmanlık Şirketi. (2016). *Bir siber saldırı yüzeyinin altında, İş etkilerine daha derin bir bakış.* ABD: Deloitte Development LLC.

enerjigunlugu.net. (2015, 09 08). *Siber Saldırılarda İlk Hedef Elektrik*. 06 28, 2020 tarihinde www.enerjigunlugu.net: https://www.enerjigunlugu.net/siber-saldirilarda-ilk-hedef-elektrik-15208h.htm adresinden alındı

Eriş, U. (2009, Kasım). Türkiye'de Kırıcı (Hacker) Kültürü. *Anadolu Üniversitesi Sosyal Bilimler Enstitüsü Doktora Tezi*, 11, 81-82. Eskişehir.

Fruhlinger, J. (2020, Nisan 20). *Kimlik avı nedir? Bu siber saldırı nasıl çalışır ve nasıl önlenir.* CSO Online: https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html adresinden alınmıştır

Garrick, B. J. (2008). Terrorist Attack on the National Electrical Grid. B. J. Garrick içinde, *Quantifying and Controlling Catastrophic Risks* (s. 111-177).

Guerrero Saade, J. A., Raiu, C., Moore, D., & Rid, T. (2018, 03). *The Dawn of Nation-State Digital Espionage.* media.kasperskycontenthub.com: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180251/Penquins_Moonlit_Maze_PDF_eng.pdf adresinden alınmıştır

İstanbul Üniversitesi Kariyer Geliştirme Uygulama ve Araştırma Merkezi. (2015). Siber Saldırı Türleri. *Bilişim'de Kariyer*(2), 12-13.

Milliyet Gazetesi. (2003, 05 28). *Batman Barajı Şifrelendi*. www.milliyet.com.tr: https://www.milliyet.com.tr/ekonomi/batman-baraji-sifrelendi-5176871 adresinden alınmıştır

Özbay, R. (2015, Aralık). Aktif Siber Savunma Teknikleri ve Performans Analizi. *Afyon Kocatepe Üniversitesi Fen Bilimleri Emstitüsü Yüksek Lisans Tezi*, 1,6,9-10,12. Afyonkarahisar.

Özkan, İ. (2019). Siber Saldırıların Ekonomik Boyutu. *Bilecik Şeyh Edebali Üniversitesi Sosyal Bilimler Enstitisü İktisat Anabillim Dalı Yüksek Lisans Tezi*, 121-122, 128. BİLECİK.

Price, P. (2019, 07 10). *Three Common Cybersecurity Scenarios and Tips for Preventing Them*. www.scmagazine.com. adresinden alınmıştır

siberbulten.com. (2018, 03 11). *Kuzey Kore'li Hackerlar 'Bankshot' ile Türk Bankalarını Hedef Aldı*. www.siberbulten.com: https://siberbulten.com/haber/kuzey-koreli-hackerlerden-turkiyeye-saldiri/ adresinden alınmıştır

STM Mühendislik Teknoloji Danışmanlık. (2019). *Siber Tehdit Durum Raporu.* Ankara: ThinkTech STM Teknolojik Düşünce Merkezi.

Şan, H. E. (tarih yok). *Prisma*. https://www.prismacsi.com/hashcat-kullanimi/ adresinden alınmıştır

Şan, H. (tarih yok). *Sızma Testlerinde Hashcat Kullanımı*. Prisma: https://www.prismacsi.com/hashcat-kullanimi/ adresinden alınmıştır

Taşdöğen, C. (2019, Aralık 27). *Siber Saldırı Nedir?* İstanbul İşletme Enstitüsü: https://www.iienstitu.com/blog/siber-saldiri-nedir adresinden alınmıştır

Uçar, O. (2015, Ocak). *Gerçek Bir Siber Saldırı Senaryosu ve Analizi.* Haziran 25, 2020 tarihinde www.slideshare.net: https://www.slideshare.net/bgasecurity/8-ocak-2015-some-etkinligi-bga-gercek-bir-siber-saldr-senaryosu-ve-analizi adresinden alındı

Ufer Media. (2019, Ocak 15). *Man In The Middle (MITM) Saldırıları Nedir?* Ufer Media: https://ufer.media/man-in-the-middle-mitm-saldirilari-nedir/ adresinden alınmıştır

wmaraci.com. (2020). *Log Nedir? Log Kaydı ve Log Tutma*. www.wmaraci.com: https://wmaraci.com/nedir/log adresinden alınmıştır

Yazıcı, M. (2015, 08 24). *İlk Modern Siber-Atak: Estonya*. http://www.tuicakademi.org/ilk-modern-siber-atak-estonya/ adresinden alınmıştır

Yiğit, T., & Akyıldız, M. A. (2014). Sızma Testleri İçin Bir Model Ağ Üzerinde Siber Saldırı Senaryolarının Değerlendirilmesi. *Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi*(18(1)), 17-19.

Yılmaz, S., & Sağıroğlu, Ş. (2013). Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri. *6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı*, (s. 158). Ankara.