SAKARYA İKTİSAT DERGİSİ CİLT 11, SAYI 1, 2022, SS. 1-16
THE SAKARYA JOURNAL OF ECONOMICS, VOLUME 11, NUMBER 1, 2022, PP. 1-16

KÖTÜ AMAÇLI YAZILIMLARIN E-TİCARET İÇERİSİNDE SİBER GÜVENLİK AÇISINDAN İNCELENMESİ

Nur Kuban Torun[1], Tolga Torun[2]

ÖZ

Ticarette ve kişisel kullanımda Internet ve Internet teknolojilerinin kullanımın artması beraberinde güvenlik konusunda endişeleri getirmektedir. Tüketiciler ve işletmeler açısından e-ticaretin yaygınlaşması bu endişelerin bertaraf edilmesi ya da en aza indirilmesi noktasında birçok araştırmanın odak noktasını oluşturmaya başlamıştır. Özellikle kötü amaçlı yazılımların kişisel bilgilere ve de ticari bilgilere ulaşmasını engelleyerek güvenli pazarlama eylemleri gerçekleştirmek adına, siber güvenlik ve siber tehdit adına farkındalık yaratmak önem arz etmektedir. Bu çalışmada Internet ortamından tüketicilerin kişisel bilgisayarlarında e-ticarete ve kişisel verilerin paylaşımına yönelik tehdit oluşturabilecek kötü amaçlı yazılımların türlerinin belirlenmesine yönelik nitel bir araştırma yöntemi ile inceleme yapılmış ve sonuçlar kaydedilmiştir.

Anahtar Kelimeler: Siber Güvenlik, e-ticaret, kişisel veri

INVESTIGATION OF HARMFUL SOFTWARES IN E-TRADE IN TERMS OF CYBER SECURITY

ABSTRACT

The increase of usage of the Internet and Internet Technologies through consumers and enterprises raises concerns about security. The widespread usage of e-commerce for consum-ers and businesses has forced to researches to focus on issues related by eliminate or minimize these concerns. It is important to increase awareness through cyber security and cyber threats, especially in order to ensure security of marketing activities by preventing malicious software from accessing personal information and commercial information. In this study, the types of harmful software that could pose a threat to the personal computers of consumers from the Internet environment was examined through qualitative research and the results were noted.

Keywords: Cyber Security, e-trade, personal data

[1] Dr. Öğr. Üyesi, Bilecik Şeyh Edebali Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, İşletme Bölümü, E-posta: nurkuban.akdemir@bilecik.edu.tr, ORCID: 0000-0002-9115-5838.

[2] Doç. Dr., Bilecik Şeyh Edebali Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü, E-posta: tolga.torun@bilecik.edu.tr, ORCID: 0000-0003-4215-406X.

1. GİRİŞ

İnternetin gündelik hayatımıza girmesiyle birlikte birçok kolaylığı beraberinde getirmiş; ancak aynı ölçüde de zararları ortaya çıkmıştır. Özellikle uzun vadeli çalışmalarda bireyselleşme, toplum dinamiklerinin değişmesi, tüketim kalıplarında yaşanan değişmeye bağlı tüketim çılgınlıkları, gelir uçurumlarının daha belirgin hale gelmesi ve internet ile bağlantılı teknolojilerin işleyişini zedeleyecek kötü amaçlı yazılımların varlığı çalışmalarca ortaya koyulmuştur. Gelişen ağ teknolojileri ve internette yaşanan değişmelerle birlikte kötü amaçlı yazılımlarla saldırılar daha tehlikeli ve daha karmaşık hale gelmiştir. Internet kullanıcıları bu zararların hepsi olmasa da genelinden haberdar olmasına rağmen yeterli önlemi almamakta ya da alamamaktadır (Karacı, Akyüz ve Bilgici, 2017:2081; Darıcılı ve Özdal, 2018:2). Dünya çapında kötü amaçlı yazılımlar vasıtasıyla yapılan kimlik bilgisi hırsızlığı şeklinde saldırılara bakıldığında ilk sırayı Amerika'nın, ikinci sırayı Rusya'nın aldığı; Türkiye'nin ise 14. sırada yer aldığı görülmektedir (Akamai, 2017). E-ticaret hacminin artması, tüketicilerin giderek sanal alışverişe yönelmesi ve nesnelerin interneti (IOT) ile birlikte tüm süreçlerin birbirine bütünleşik olmasıyla siber saldırılar gelişmiş ülkelerin gündeminde yer edinmekte ve siber güvenlik politikaları oluşturma gereği duyulmaktadır. Ancak bu durum ülkemizde yeni yeni varlığını hissettiren bir durum olmuştur (Göztepe, vd. 2014:6). Türkiye'de siber güvenlik çalışmalarının hız kazanmasında en önemli adım, Bakanlar Kurulu'nun 2012 yılında aldığı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna ilişkin Kararı" ile olmuştur. Bu kararın amaç ve kapsamı, "kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda yer alan sistemlerin güvenliğinin sağlanmasına ve gizliliğinin korunmasına yönelik tedbirlerin alınması ve bilgi ve iletişim teknolojilerine ilişkin kritik altyapıların işletiminde yer alan gerçek ve tüzel kişilerce uyulması gerekli usul ve esasların düzenlenmesidir" ifadesinde yer almaktadır (Resmi Gazete, 2012). Türkiye siber güvenlik yönetiminde devlet kurumlarının eş güdümünün yanı sıra sivil toplum kuruluşları, üniversiteler ve özel sektörün iş birliğiyle oluşturacağı ekosistem Türkiye'nin teknoloji ihracatı, diplomatik etkinliği, istihbarat gücü, siber alandaki menfaatlerinin korunması gibi birçok önemli konuda ilerlemesinin yolunu açılması hedeflenmektedir (Tubisad, 2017). 2016-2019 Belgesinde 5 stratejik ana eylem planı yer almaktadır:

1- Siber Savunmanın Güçlendirilmesi ve Kritik Altyapıların Korunması
2- Siber Suçlarla Mücadele
3- Farkındalık ve İnsan Kaynağı Geliştirme
4- Siber Güvenlik Ekosisteminin Geliştirilmesi
5- Siber Güvenliğin Milli Güvenliğe Entegrasyonu (2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, 2016).

1.1. Siber Güvenlik ve Terörizm Kavramı

Güvenlik Türk Dil Kurumu Sözlüğü'nde "Toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet."

(TDK, 2019) olarak tanımlansa da güvenlik konularını ele alan çalışmalarda ve devlet raporlarında güvenliğin bakış açılarına göre değiştiği ve buna göre tanımladıkları görülmektedir (Bayraktar, 2014:1300). Teknik anlamda güvenlik, "insanların, eşya ve maddelerin, araç ve bilgilerin tehlike ve tehditlerden uzak olma, güven, huzur ve sağlık içinde bulunmasını tehdit eden, zarara ve hasara veya faaliyet ve işlev ya da görevinden men etmeye veya kısıtlamaya, baskı, cebir, şiddet, şantaj veya herhangi bir eylemle onu istenmeyen durumlara yönlendirmek için yapılan işleri durdurmaya, engellemeye, caydırmaya veya etkisini en aza indirmeye yönelik plan, program ve prosedürlerle belirlenen etkinlikler sonucu arzulanan durumun oluşturulmasıdır" (Bal, 2003:65). Güvenlik, kişilerin, ailelerin, sivil toplum kuruluşlarının ve güvenlik örgütlerinin ortaklaşa üstlendikleri bir olgudur. Güvenlik, kişilerin canına, namusuna ya da mallarına gelebilecek tehditlerin bertaraf edilmesi olarak tanımlanabilmektedir. (TODAİE, 1992:229). Güvenlik içerisinde tehdit unsuru böylelikle en önemli kavram olarak ortaya çıkmaktadır.

Güvenlik ve tehdidin geçmişini milattan önce zamanlara kadar götürmek mümkündür. Hitit ve Mısır arasında yaşanan güvenlik-tehdit unsuru, antin Yunan döneminde devam etmiş, Roma uygarlığı bu süreci izlemiş ve 15. Yüzyıl ve 19. Yüzyılda Modern Çağ içerisinde bu iki kavram büyük değişmelere uğramıştır. Modern Çağ'da bilim ve teknolojinin ortaya çıkması güvenlik ve tehdidin niteliğini değiştirmiştir. 20. Yüzyılın başlarında güvenlik ve tehdit kavramlarına ideolojilerin yayılması da eklenmiştir. Özellikle 2. Dünya savaşı sonrasında ABD ve SSCB ikili bir kutup yaratarak soğuk savaş dönemine girmiş ve güvenlik ve tehdit anlayışında değişmelere sebebiyet vermişlerdir (Bayraktar, 2015: 28-29). Özellikle Internet teknolojilerinin yaygınlaşması ile birlikte biyolojik silah ve siber terörizm gibi yeni tehditler ortaya çıkmıştır. Siber terörizm, bilgisayarlarla, internet üzerinden birçok gizli bilgiye ulaşılarak siyasi otoriteyi güçsüzleştirmek ya da halkı provoke edecek bilgileri yayarak kargaşa çıkarmak şeklinde tanımlanmaktadır. Siber terörizmin işleyişi dijital bir savaş şeklinde olmaktadır. (Denning, 2001). Türkiye'de siber güvenlik kapsamında riskler 10 madde halinde belirlenmiştir. Bu maddelerin odak noktası siber terörizm neticesinde hizmetlerin kesintiye uğraması, bilgilerin ele geçmesi, propaganda yapılması, maddi kayıplar ve kötü amaçlı yazılımlardır (http://www.udhb.gov.tr).

1.2. Siber Güvenlikte Kötü Amaçlı Yazılımlar

Siber güvenlik kapsamında terörizm amacıyla geliştirilen birçok kötü yazılım türü bulunmaktadır. Bu kötü yazılımlar aşağıdaki şekildedir.

IP Sahtekârlığı (IP Spoofing): IP sahtekârlığı, birçok ağın, veri alışverişinde giden trafiğine kaynak IP filtresi uygulamadığından dolayı, saldırganın isteğe bağlı bir kaynak IP adresi eklemesinden kaynaklanmaktadır. Ip sahtekârlığında, gizlenmiş kimlik sayesinde tarayıcıya sızılmakta veya ağ oturumları sayesinde kaynaktaki bilgiye ulaşılmaktadır. IP sahtekârlığında, sahte birçok bağlantı oluşturularak ve

gerçek saldırının kaynağı gizlenerek hedefin güçsüz hale getirilmesi amaçlanmaktadır (Kovacik vd. 2013:2).

Kötü Amaçlı Yazılım (Malicious Program): Kötü amaçlı yazılım, normal sistem işlevlerini bozmak için kullanılan, önemli bilgileri toplayan veya kötü amaçlı yazılım da denilen özel bilgisayar sistemlerine erişebilen ve kodlama, komut dosyaları, etkin materyal vb. şeklinde olabilen herhangi bir yazılımdır. Çeşitli düşmanca veya müdahaleci yazılım biçimleri için kötü amaçlı yazılım terimi kullanılmaktadır (Schultz, vd. 2001:39). Kötü amaçlı yazılımlar, kötü amaçlı yazılım tarayıcılarını veya güvenlik amacıyla yüklenen virüs tarama programlarını devre dışı bırakmak gibi çok fazla etkinlikleri olduğu için tehlikelidir. Dünya'da "I love You" virüsü 45 milyon bilgisayara ulaşmış ve 10 milyar dolarlık zarara neden olmuştur. Bunun dışında bilinen Nimda, MyDoom ve Sapphire/Slammer adlı kötü amaçlı yazılımlar da kullanıcılara zarar vermiş ve bilgisayar tamir ve bakım masraflarına son yıllarda yüksek meblağlar ödenmeye başlanmıştır (Ünver ve Canbay, 2015:96).

Kötü amaçlı yazılımlar genel olarak aşağıdaki şekilde kategorilere ayrılabilir.

a- Virüsler

Virüs, internette kendini tekrar eden birçok zararlı etkiye sahip bir programdır. İlgili kodu çalıştırdığımızda, bu programlar otomatik olarak yürütülür. Virüsler, kendilerini değiştirerek modifiye edebilirler. Bu programlar, herhangi bir bilgisayardan diğer bilgisayarlara ağ üzerinden veya USB aygıtlarından yayılabilir. Ana hedef, MSDOS ve sabit diskteki, genel amaçlı komut dosyasındaki ikili çalıştırılabilir dosyalardır (Cohen, 1987:22).

b- Solucanlar

Solucanlar, art arda meydana gelen programlar ve farklı veri kümelerini kullanıcı yetkisi olmadan diğer sistemlere aktaracak ağa sahiptir ve kopyalar kendiliğinden oluşturulur. Solucanlar, bant genişliğini veya frekans bantlarını kullanarak genel ağı etkileyebilir. Gizli virüs saldırısı veya önemsiz e-posta saldırıları gerçekleştirdiğinde dosyaları şifreleyebilir ya da silebilir (Jain ve Bajaj, 2014: 931).

c- Spyware

Casus yazılım, yakın zamanda ziyaret edilen web sayfaları, e-postalar, ATM numarası vb. Gibi müşteriyle ilgili kişisel bilgileri izleyip toplayabilen sistemin yazılımıdır. Herhangi bir ücretsiz veya deneme yazılımı indirilirken otomatik olarak yüklenebilmektedir (Jain ve Bajaj, 2014: 931).

d- Adware

Kötü amaçlı yazılımlar indirildikten veya herhangi bir uygulama kullanıldıktan sonra otomatik olarak oynatılan, gösterilen ve hatta sisteme indirilen reklam şeklindedir. Adware, yazılıma gömülü bir kod parçasıdır. Bu tip reklam yazılımlarında amaç kullanıcıların, internetteki etkinliklerini kontrol etmektir (Jain ve Bajaj, 2014:931).

e- Trojanlar (Truva Atları)

Trojanlar, uzaktan erişim olanağı sağlayacak şekilde kullanıcı isimlerini ele geçiren ya da şifreleri deşifre eden programlar şeklindedir. Bu yazılımlardan bazıları, sisteme zarar verebilecek ve hizmetleri sekteye uğratacak yapıya da sahiptir (Thuraisingham, 2005:3).

f- Botnet

Botnet, kendi kendine hareket edebilen robot yazılımlar sayesinde uzaktan kontrole olanak sağlayan yazılım çeşitleridir. Bu yazılımlar genellikle güvenli ağ veya ortak kontroller ile denetimi sağlanan zombi programlardır. Bunlar spam spyware göndermek amacıyla kullanılmaktadır. Botlar çalışmak için üçüncü şahıslara ihtiyaç duymaz ve yüzlerce bot birbirleriyle hiyerarşik bir yapı oluşturarak iletişime geçip otomatik olarak çalışabilirler (Jain ve Bajaj, 2014:932).

1.3. E-Ticaret ve E-ticaret ile Bağıntılı Unsurlarda Siber Güvenliğin Önemi

Internet teknolojilerinin yaygınlaşması ve tüketicilerin artık dijital kimlik kazanarak e-ticaret ve sosyal medya mecralarında yer bulmasıyla birlikte, pazarlamaya konu olan değiş/tokuşların bu alanlara taşınması kaçınılmaz olmuştur. Günümüzde bu değişim ilişkilerinin hacmi milyar dolarlar ile anılmaktadır. Ancak sadece değişim ilişkileri olumlu bir yönde değil; kişisel bilgilerin merdiven altı pazarlanması ve dolandırıcılığa konu olacak şekilde bilgilerin elde edilmesi şeklinde olumsuz bir şekilde de kendisi göstermektedir. Bu açıdan siber güvenliğin, özellikle elektronik ticaret ve e-ticaret ile ilişkili unsurlar açısından ele alınması önem arz etmektedir. İnternet bankacılığı, kredi kartları ve kişisel bilgiler e-ticaret ile bağıntılı unsurlardır.

1.3.1. Siber Güvenlik ve E-Ticaret

Elektronik ticaret, dijital veya fiziksel olarak teslim edilebilen; tüketicileri, firmaları ve hükümetleri kapsayan mal ve hizmet ticaretinde dijital olarak etkinleştirilmiş işlemler bütünü olarak tanımlanmaktadır (González ve Jounjean, 2017:4). E-Pazar diye nitelendirilen elektronik ticaretin hüküm sürdüğü pazarlarda Amazon ve Alibaba gibi güçlü siteler bulunmaktadır. Ayrıca e-ticaret sosyal medya üzerinden de oluşmaya başlamıştır. 2018 yılında gerçekleşen e-ticaret hacmi 189 milyar dolardır (Abrams, 2018). E-ticarete dâhil olan işletmeler için kişisel bilgilerin korunması, saklanması ve 3. şahıslarla onay olmadıkça paylaşılmaması noktasında zorunluluklar çıkmaktadır. Bu amaçla işletmelerin, saldırılara ve tehditlere yönelik önlemlerini alması gerekmektedir (Özmen, 2013). Stratejik ve Uluslararası Araştırmalar Merkezi – CSIS araştırmasına göre malware ve malicious gibi yazılımlarla ve phishing ile işlenen siber suçlar yüzünden işletmelerin zararı 600 milyar dolardır (Lewis, 2018). 2021 yılında yapılan araştırmalara göre, 2020 yılında e-ticaret sitelerine yönelik yapılan siber saldırılar %56 oranında artmıştır. E-ticaret sitelerinden özellikle %33'ü ödeme bilgilerini elde etmeye yönelik saldırılar olmaktayken %27 kişisel veriler ve %20 kimlik bilgilerini elde etmeye yönelik saldırılar yapılmaktadır (DHA, 2021).

1.3.2. Siber Güvenlik ve Internet Bankacılığı

Bilişim teknolojileri, bankacılık alanında da kendisini göstererek Internet bankacılığı ya da çevrimiçi (online) bankacılık denilen sistemi oluşturmuştur (Sohail ve Shanmugham, 2003:210). Yeni teknolojilerin kolay ve hızlı bir şekilde adapte edildiği bankacılık sektöründe, bilgisayar ile bankacılık işlemlerinin yapılması 1990'lı yıllardan bu yana süregelmektedir. Ancak Internet bankacılığında, bilgisayarların ya da yeni nesil cep telefonlarının kullanılması aynı zamanda tüketicilerde güvenlik endişesi yaratan bir diğer unsurdur (Barışık ve Temel, 2007:139). Internet bankacılığı büyük riskleri de beraberinde getirmektedir. Güvenlik riskleri şeklinde tanımlanabilecek bu risklerin en önemlisi kişisel bilgilerin ele geçirilmesi ve kişilerin hesaplarına kötü niyetli 3. şahısların ulaşmasıdır (İçli Eti ve Aslan, 2008:113). Bilgisayarlar içerisine yerleştirilen korsan yazılımlar ya da casus yazılımlar vasıtasıyla, hesap sahiplerinin bilgileri ve hesapları üzerinde kötü niyetli kişilerin hâkimiyeti kurulabilmektedir (Bilgen, 2009:78). 2021 yılında Alman Deutsche Bank AG'ye yönelik bir siber saldırı olmuş ve bu siber saldırı engellenmiştir. Türkiye'de ise Akbank'ta 35 saatlik bir kesinti yaşanmış ve gündeme siber saldırı sorusunu getirmiştir. Akbank tarafından siber saldırı doğrulanmamıştır..

1.3.3. Siber Güvenlik ve Kredi Kartları

Malwar e gibi kötü yazılımlar, kredi kartları bilgilerine erişim sağlamakta ve kredi kartlarını gerek maddi olan dolandırmakta gerekse kişilerin kart bilgilerinden menfaat sağlamaktadır. Dünya üzerinde 40 milyon kredi kartı kullanıcısının kart bilgilerinin korsanlar tarafından çalınmış olma riskinin bulunduğu raporlarda belirtilmiştir (Pigni vd. 2018:9). Özellikle Internetten alışveriş sırasında kullanılan kartların, maddi kayıplarla sonuçlanan korsan saldırılarına maruz kaldığı bilinmektedir (Epstein ve Brown, 2008:207). Kredi kartları ile doğrudan ödeme noktasında sorunların ortadan kalkması amacıyla dijital cüzdanlar geliştirilmiştir. Ancak dijital cüzdanların da tam bir koruma sağlamadığı bilinmektedir. Özellikle doğum tarihi, adres, TC kimlik numarası gibi kişisel bilgileri içeren fatura şeklinde e-mailler ile kişiler ödeme yapmaya sevk edilmekte ve banka bilgileri phishing (oltalama) şeklinde ele geçirilmektedir. Ayrıca kullanıcılar, kötü amaçlı URL uzantılarına tıklatılmak suretiyle kart bilgilerini girmesiyle dolandırıcılığa maruz kalabilmektedir (Enisa, 2016).

Kredi kartı dolandırıcılığını çevrimiçi kredi kartı sahtekârlığı ve çevrimdışı kredi kartı sahtekârlığı şeklinde ikiye ayırabilmekteyiz (Al-Khatib, 2012:137). Çevrimiçi kredi kartı sahtekârlığı Internet üzerinden yapılan alışverişler için, bilgileri ele geçirilen kartların kullanılması şeklinde olmaktadır. Çevrimdışı kredi kartı sahtekârlığı ise çalınan veya taklit edilen bir kredi kartının fiziksel bir mağazadan ürün veya hizmet satın alım işlemi için kullanılmasıdır. Çevrimiçi kredi kartı sahtekârlıklarında, bir kredi kartı bilgilerinin çalındığı veya bazı durumlarda geçerli kredi kartı bilgilerinin hackerlar tarafından oluşturulduğu durumdur. Çevrimiçi kredi kartı sahtekârlıklarda, kartın bilgilerini ele geçirmeye yarayan kötü amaçlı yazılımlardan ve tekniklerden yararlanılmaktadır (Akhilomen, 2013:1). Euronews

(Can, 2019) haberine göre Türkiye'de 460 bin kredi kartı bilgisi çalınmış ve karaborsada satılmaktadır. Bu piyasanın değeri 500 bin doların üzerindedir. Bu hırsızlığın yemleme, zararlı yazılım ya da Java-Script yazılımı üzerinden sızma ile yapılmış olabileceğini ve kart bilgilerinde e-posta ve telefon bilgilerinin de yer alması nedeniyle hırsızlığın POS cihazları üzerinden yapılmış olma ihtimali de düşünülmektedir.

1.3.4. Siber Güvenlik ve Kişisel Bilgiler

Günümüzde tüketicilere birebir olarak ulaşmak önem kazanmıştır. Bu yüzden firmalar için e-postalar üzerinden tüketicilere bilgilendirme ya da tanıtım içeren mesajların atılması özellikle tüketiciye ulaşmada kullanılan yaygın bir yöntem olmuştur. Ancak çoğu zaman bu e-postalar tüketiciler bilgisi ve de rızası dışında ulaştırılmaktadır. İstem dışı atılan e-postalar spam olarak nitelendirilmektedir (O'Reirdan, 2011:17). Bu konuyla ilgili Türkiye'de bir çalışma başlatılmış ve 15 Temmuz 2015 tarihli Resmi Gazete'de kişilere internet yoluyla ulaşmanın hükümleri belirlenmiştir. Buna göre "Hizmet sağlayıcının, mal ve hizmetlerini tanıtmak, pazarlamak, işletmesini tanıtmak ya da kutlama ve temenni gibi içeriklerle tanınırlığını artırmak amacıyla alıcıların elektronik iletişim adreslerine gönderdiği ticari elektronik iletiler için kendisi tarafından önceden onay alınır. Onay, reddetme hakkı kullanılıncaya kadar geçerlidir." ibaresi koyulmuştur (Resmi Gazete, 2015). Ayrıca e-posta bir dolandırıcılık aracı olarak da kullanılabilmektedir. Mevcut bir websitesinin klon (kopya) hali tüketiciye gönderilerek, tüketicinin giriş yapması sağlanmakta ve bu sayede tüketicilerin kişisel bilgilerine ulaşılabilmektedir. Bu yöntem oltalama/clickbait denen bir dolandırıcılık şeklidir (SOME, 2019). 2021 yılında online yemek sipariş sitesi olan Yemeksepeti.com siber saldırıya uğrayarak, kullanıcıların kayıtlı telefon numaraları, adres bilgileri, e-posta adresi gibi kişisel bilgilerinin çalındığı ortaya çıkmıştır. Bu bilgilerle hedefli oltalama yönetmi denilen dolandırıcılık türünün yapılması muhtemeldir.

2. YÖNTEM

Günümüzde e-ticaret hacminde büyük artışlar yaşanmaktadır. Özellikle 25-44 yaş aralığında bireylerin e-ticareti kullanma oranları yüksektir. Türkiye'nin 2020 e-ticaret hacmi 91,7 milyar TL olup 83,3 milyar TL'lik kısmı yurt içi harcamalar şeklinde kendini göstermektedir. 2019 yılından beri e-ticaret hacmindeki artış %64 olarak ifade edilmektedir. Ödeme yöntemleri itibari ile incelendiğinde kartlı işlemler 58,1 milyar TL, havale/eft 30,1 milyar TL ve kapıda ödeme ise 3,4 milyar TL'lik paya sahip olduğu görülmektedir (eticaret, 2021). E-ticaret hacminin artması ve özellikle kartlı işlemlerin yaygınlaşması beraberinde tehditleri de getirmektedir. Ancak Türkiye'de bu tehditlere yönelik artışa rağmen, keşfedici çalışmaların sayısının yetersizliği Bilgi Teknolojileri ve İletişim Kurumu'nun 2018 yılında düzenlediği Siber Güvenlik Ekosisteminin Geliştirilmesi adlı zirvede belirtilmiştir (Sibergüvenlikzirvesi, 2021). Bu kapsamda, araştırmada bedava yazılım, program, oyun ve dizi/film izleme olanağı sağlayan web sitelerinde hangi tür zararlı

yazılımların yer aldığının tespit edilmesi amaçlanmıştır. İnternette yer alan bu tarz uygulamalar sunan web sitelerinin ürünü, kullanıcılarına sağladığı bedava ayrıcalıklardır. Bu ayrıcalıklar çoğu zaman telif haklarının ihlali gibi yasal olmayan bir zemin üzerine kuruludur. Ancak özellikle maddi kaygılardan dolayı birçok kullanıcı bu tür web sitelerine rağbet edebilmekte ve maalesef bilgisayarlarına kötü amaçlı yazılımları davet etmektedir. Bunun sonucunda elektronik pazarlamanın arttığı dijital çağda kişisel verilerin izinsiz kullanımı ve maddi kayıplar oluşabilmektedir.

Araştırmada nitel araştırma yöntemlerinden birisi olan keşfedici yöntem kullanılmıştır. Bu yönteme göre problem e-ticaret ve kişisel veriler açısından tehdit yaratan kötü yazılımların türlerinin tespiti olarak belirlenmiştir. Araştırma kapsamında kişilere bedava yazılım ve uygulamalar sunan websiteleri, e-mail gönderileri, flashbellekler, cd gibi yükleme esasına göre çalışan unsurlar anakütleyi oluşturmaktadır. Anakütle içerisinden örneklem belirlenmesi amacıyla Google Analitik içerisinde en çok arama yapılan uygulama indirmeye yarayan web siteleri incelenmiş ve incelemeye olanak veren 6 adet web sitesi örneklem olarak ele alınmıştır. Verilerin toplanması amacıyla bu web sitesinde yer alan programlar ve dizi/film izlemeye yönelik uygulamalar kişisel bilgisayarlara indirilerek çeşitli kötü amaçlı yazılım tespit programları ile incelenmiş ve sonuçlar kaydedilmiştir. Bulgularda bahsi geçen kötü amaçlı yazılımların tespit edilen isimleri taramanın yapıldığı koruma programları tarafından atanan isimler olabilmektedir. Bu açıdan isimlerin virüs olup olmadı; eğer virüs ise hangi tür virüslere dahil edilebileceği sonuçlar bölümünde değinilmiştir. Araştırmanın bu anlamda en büyük kısıtı henüz tespit edilememiş yazılımların adlandırılamaması ve hangi tür kötü amaçlı yazılım olduğunun belirlenememesidir. Araştırmaya dahil edilen web sitelerinin isimleri kullanıma teşvik olamaması amacıyla ve isim hakları sebebiyle verilmemiş, onun yerine web1, web2, web3, web4, web5 ve web6 olarak kodlanmıştır. Web1'in aylık ziyaretçi sayısı 8.14 milyon kişi olup, ziyaretçilerin %64,8'i araştırarak, %33,6'sı ise doğrudan sayfayı bulmaktadır. Web2'in aylık ziyaretçi sayısı 2.98 milyon olup %62.05'i araştırarak, %35,04'ü doğrudan ve %2,46'sı sosyal ağlardan siteye ulaşmaktadır. Web3'ün aylık trafiği 2.32 milyon olup %85,28'i araştırarak, %11,56'sı doğrudan ve %3,16'sı sosyal ağlardan siteye ulaşmaktadır. Web4'ün aylık trafiği 2.11 milyon olup %75,28'i araştırarak, %22,53'sı doğrudan ve %2,19'sı sosyal ağlardan siteye ulaşmaktadır. Web5'in aylık trafiği 3.32 milyon olup %83,24'i araştırarak, %13,60'sı doğrudan ve %3,16'sı sosyal ağlardan siteye ulaşmaktadır. Web6'nın aylık trafiği 4.21 milyon olup %85,48'i araştırarak, %11,32'sı doğrudan ve %3,20'sı sosyal ağlardan siteye ulaşmaktadır

3. BULGULAR

Web1'de en çok indirilen 52 adet oyun amaçlı program belirlenmiştir. Bu belirlenen programlar bilgisayarlara indirilerek, çeşitli kötü amaçlı yazılım tespit programları ile taranmış ve 29 tanesinde kötü amaçlı yazılım tespit edilmiştir. İndirilen programların içerdiği kötü amaçlı yazılımlar FileRepMalware (PUP),

Trojan.InstallCore.3432, Malicious, PUP.Optional.InstallCore.Generic, DealPly, Virus.Win32.Gen.ccmw, Adware.InstallCore!1A30C, Heuristic, Malicious.confidence.90%, Application.Generic (A), Win32/InstallCore.Gen.A ve PUA:Win32/InstallCore'dur. Tespit edilen kötü amaçlı yazılımlara bakıldığında malware, trojan, PUP, dealply ve trojan ağırlıklı kötü amaçlı yazılımlar olduğu görülmektedir.

Web2'de 50 adet bilgisayar programı indirilerek çeşitli kötü amaçlı yazılım tespit programında taranmış ve 33 tanesinde kötü amaçlı yazılıma rastlanmıştır. İndirilen programların içerdiği kötü amaçlı, Trojan.win32, malware, Tool.arp9, riskware.win32, Bscope.Trojan, Trojan.Generic, Trojan.Agentdt, Heuristic, suspicious_gen, Adware.crossrider, W32/Genplus, Tool.ultra.surf.17, PUA.UltraReach, Trojan.VBKrypt.Win32, Trojan.Zapchast.win32, Win32:PSWTool(PUP), FilerepMetagen (PUP), Artemis, UDS:DangerousObject, Unsafe, Nirsoft.smartsniff, backdoor ve packed.dico'dur. Programlardan yayılan kötü amaçlı yazılımlara bakıldığında, trojan, solucan, casus yazılım, makro, adware, casus çerez, back door, malware ve tarayıcı ele geçiriciler olduğu görülmektedir.

Web3'te, en çok indirilen 35 program ve 15 oyun inceleme altına alınmıştır. Programlardan 34'ünün, oyunlardan ise 7'sinin kötü amaçlı yazılım taşıdığı görülmüştür. Bu kötü amaçlı yazılımlar, hacktool, win32.tiggre!rfn, win32/Bluteal!rfn, win32/Zpevdo.A, win32/Fuerboos.C!cl, FileRepMalware (PUP), applicationdealaplha.1.gen, malicous, trojan.Installcore, dealply, malware_confidence, unsafe, heuristic, mlattributehighconfidence, riskware, PUPOpt,onal.InstallCore.generic ve virus.win32.gen.ccmw'dur. Tespit edilen kötü amaçlı yazılımların malware, trojan, dealply, malicious ve unsafe olduğu görülmektedir.

Web4'te 62 adet oyun amaçlı program incelenmiş ve sadece 7 tanesinde kötü amaçlı yazılım tespit edilmiştir. Bu yazılımlar malware tarzı kötü yazılımlardır.

Web5'te, 51 adet program incelenmiş ve 6 tanesinde kötü amaçlı yazılım tespit edilmiştir. Bu kötü amaçlı yazılımlar, webtoolbar.Js.condonit.a, UDS:dangerousobject.multi.generic, HEUR:downloader.win32.driverpack.gen, risktool,win32 ve UDS:adware.win32'dir. Kötü amaçlı yazılımlar genel olarak trojan, reklam yazılımı ve heuristictir.

Web6'da 34 adet program incelenmiş ve 30 tanesinde kötü amaçlı yazılıma rastlanmıştır. Bulunan kötü amaçlı yazılımlar, filerepmetagen, win32:Malware-gen, filerepmalvare(PUP) ve win32.Installcore'dur. Kötü amaçlı yazılımlara bakıldığında malware ve reklam amaçlı yazılımlar olduğu görülmektedir.

4. SONUÇ

Internet ve bilişim teknolojileri insanların ve de işletmelerin hayatına birçok olumlu katkı sağlasa da aynı zamanda birçok olumsuz ve istenmeyen durumu da getirmiştir. Özellikle Internet üzerinden elde edilen programlar vasıtasıyla bilgisayarlar kötü amaçlı yazılımların etkilerine açık kalmakta ve birçok bilgisayar

kullanıcısı gerek elektronik ticaret esnasında gerekse çevrimiçi bankacılık sırasında bilgilerinin ele geçirilmesi tehdidi ile karşı karşıya kalmaktadır. Her ne kadar kötü amaçlı yazılımların önlenmesi amacıyla birçok koruyucu program piyasada bulunsa da, kötü amaçlı yazılımlar bağışıklık kazanmak adına kendilerini yenileyerek tekrardan yayılmaya hazır bir şekilde Internet ortamında bulunabilmektedir.

Çalışmada güncel oyunları, bedava sunulan ya da korsan olarak illegal paylaşılan bilgisayar programlarını içeren ve dizi/filmleri izlemeye yarayan en çok rağbet gören 6 adet web sitesi inceleme altına alınmıştır. Bu web sitelerinden indirilen gerek oyun gerekse programlarda büyük ölçüde kötü amaçlı yazılımlar tespit edilmiştir. En çok tespit edilen kötü amaçlı yazılım şekli malware yazılımlarıdır. Bu tür yazılımlar casusluk ve bilgi elde etmek amacıyla kullanılmaktadır. Bu yazılımların bulaştığı bilgisayarın hangi web sitelerine girdiği, neleri araştırdığı ya da hangi bilgileri girdiği deşifre edilmektedir. Özellikle bu tür yazılımlar bankacılık işlemleri için tehdit oluşturmaktadır. Diğer önemli kötü amaçlı yazılım şekli ise trojanlardır. Trojanlar siber hırsızlık amacıyla korsanlarca kullanılır ve sisteme ulaşma amacı taşımaktadır. Trojanlar, bulaştığı ağlar arasında bir zombi ağı kurarak siber suçlar işleyebilir. Ayrıca kişilerin banka ve de şifre gibi kişisel bilgilerini çalmak amacıyla kullanılmaktadır. PUP ya da PUA (potentially unwanted application/potansiyel istenmeyen uygulama) bilgisayarlarda tarayıcı üzerinde değişiklik yapmaya yarayan kötü amaçlı yazılımlardandır. Bu yazılımlar ayrıca kullanıcıların rızası dışında reklam gösterimi de yapabilmektedir. DealPly, reklam göstermeye yarayan bir kötü amaçlı yazılımdır. Aynı zamanda kişilerin bilgilerini elde ederek karşı tarafa iletir. Malicious software bilgisayar sistemine zarar vermek ve de kişisel bilgileri çalmak amacıyla kullanılan kötü amaçlı yazılımlardandır.

FileRepMalware (PUP) adlı kötü amaçlı yazılım bir trojandır ve genelde e-postalar ile bilgisayarı infekte etmektedir. Bu dosyaların uzantıları vbs., .exe ve benzeri uzantılardır. Eğer bu uzantıya sahip bilinmeyen ve şüpheli bir e-posta varsa bu tür bir kötü amaçlı yazılım olması muhtemeldir. Bu yazılımların amacı bilgisayarlarda arka kapı oluşturması ve uzaktan erişime imkân tanımasıdır. Özellikle siber suçluların bilgisayarlara ulaşmasına olanak tanıması açısından zararlı bir yazılımdır. Ayrıca bu tür yazılımlar, bilgisayarlara izinsiz ek yüklemelere de izin vermektedir.

Trojan.InstallCore.3432 ve Adware.InstallCore!1A30C adlı kötü amaçlı yazılımlar, bilgisayar işleyiş kalitesini düşürücü bir niteliğe sahiptir. Bu tür trojanlara sahip bilgisayarların, kullanıcının kontrolü dışında davranışlara sahip oldukları görülmektedir. Ayrıca bu trojanlar, tarayıcılara eklenmekte, tarayıcı ayarlarını değiştirmekte, kısayollar üzerinde etkili olmakta, tarayıcılara izinsiz uzantılar yüklemekte, kullanıcı erişim kontrolünü devre dışı bırakmakta ve araç çubukları üzerine reklamlar oluşturmaktadır (Microsoft, 2019).

Malicious kötü amaçlı yazılımları, bilgisayar sistem güvenliğini tehdit eden önemli bir yazılımdır. Bu yazılım bilgisayarlara izinsiz girişler için imkân

sağlamaktadır. Günümüz koruma programları bu tür yazılımları tespit noktasında çalışsa da engelleme noktasında yetersiz kalmaktadır (Ray ve Poolsappasit, 231).

Kötü amaçlı yazılımlar içerisinde tespit edilen PUP.Optional.InstallCore.generic yazılımı da bir tür malware yazılımdır. Bilgisayarlara genelde bir dosya indirilirken bildirim yapılmadan habersizce yerleşir. Bu yazılımın en büyük tehdit oluşturduğu nokta, kullanıcının haberi olmadan birçok başka kötü amaçlı yazılımın girişine izin vermesidir. Bu yazılımlar bedava programlarda ya da paylaşım sitelerinde sunulan ürünlerde bulunmaktadır. Kullanıcıların tarayıcılarını hedef alarak bu tarayıcıları ele geçirir. Pop-up reklamlara olanak tanımakta ve hatta tarayıcı ayarları üzerinde değişiklikler yaratmaktadır (Malwarefixes, 2019). Diğer bir reklam olanağı sağlayan kötü amaçlı yazılım Adware.CrossRiderdır. Bu yazılım dosyalara yapışık şekilde bilgisayara sızmakta ve reklam uzantılarını açarak 3. Şahıslara tıklama şeklinde reklam geliri elde etme noktasında yardım eder.

Dealply trojan şeklinde bir kötü amaçlı yazılımdır. Bu yazılım hackerların bilgisayarına erişimini kolaylaştırmaktadır. Ayrıca hackerların komutlarını, bulaştıkları bilgisayarda yerine getirmektedir. Diğer bir trojan ise Virus.Win32.Gen.ccmw adlı kötü amaçlı yazılımdır. Bu yazılım türü Windows çalıştırılabilir dosyalarına ve HTML uzantılı dosyalara bulaşmakta ve çıkabilir sürücülere yayılabilen virüs tipidir. Bu yazılımlar arka kapı oluşturmakta ve hackerlardan komutlar almaktadır (Microsoft, 2019).

Taramalardan çıkan bir isim de Malicious.confidence.90%'dır. Koruma programları tarafından verilen bir kod olan Malicious_confidence_90% (D), bir Truva Atı'nı genel olarak tespit etmek için tasarlanmış bir sezgisel algılamadır. Bu tarz trojanlar diğer kötü amaçlı yazılımları indirmekte, bilgisayarlarda tıklama sahtekârlığı için kullanılmakta, tuşlanan şifreleri ve ziyaret edilen sayfaları kaydetmekte ve hackerlara göndermekte, bilgisayarları erişime açmakta, izinsiz reklamlar açmakta ve sahte güncellemeler oluşturarak kullanıcının rızası dışında yüklemelere olanak sağlamaktadır (Microsoft, 2019).

Application.Generic (A) adlı kötü amaçlı yazılım ek güvenlik riskleri doğurabilecek şekilde uzaktan yönetime izin veren, dosya aktarmaya yarayan ve bilgisayardaki verileri sızdıran bir kod şeklidir. Bir diğer kötü amaçlı yazılım ise Suspicious_GEN trojanıdır. Siber suçlular tarafından tasarlanmış bir yazılımdır. Bilgisayarın sistem dosyalarında değişiklikler yapmakta ve tarayıcıyı kullanıcının bilgisi dışında sitelere yönlendirmekte ve izinsiz şekilde reklamlar açmaktadır.

Trojan.Zapchast.win32 hackerlara bilgisayarlarda arka kapı açan ve hackerların bilgisayarları kontrol etmesine yarayan bir trojan türüdür. FilerepMetagen bilgisayarlarda kullanıcının kontrolü olmaksızın reklam açan virüs türlerindendir. Win32/Fuerboos.C!cl, Backdoor ve packed.dico kötü amaçlı yazılımı hackerların bilgisayarlara sızmak için kullandıkları trojandır.

Sonuç olarak dosya ve oyun paylaşım ve dizi/film izleme web sitelerinden sağlanan ücretsiz hizmetlerin beraberinde birçok programın kötü amaçlı yazılım içerdiği görülmektedir. Genel olarak bu kötü amaçlı yazılımlar malware, trojan ve maliciouslardır. Virüs programları bu kötü amaçlı yazılımlara veri tabanında yer alan örneklere göre isimler vermektedir. Ancak bazı durumlarda özellikle tehdit oluşturan unsurun yeni olduğu durumlarda kötü amaçlı yazılım tespit programları dahi bu yazılımları belirlemede yetersiz kalabilmektedir. Kullanıcılar çoğu zaman farkına varmadan ya da elde edecekleri dosyanın önemine bağlı olarak risk alarak bu yazılımları bilgisayarlarına indirerek kişisel bilgileri ele geçirilmekte ve maddi kayıplarla karşılaşabilme ihtimallerini arttırmaktadır.

Görüldüğü üzere dosyalara yapışık olarak gelen trojanların ve diğer kötü amaçlı yazılımların klavye hareketlerini ve girilen bilgileri kaydetme ve 3. taraflara gönderme özelliği bulunmaktadır. Dünyada perakende elektronik ticaret hacminin 2,4 trilyon dolar ve Türkiye'de 60 milyar TL olduğu bir pazar gerçekliği bulunmaktadır. Çoğu uluslararası ve hatta ulusal marka fiziksel dükkanları kapatma aşamasına gelerek Internet ortamlarına taşınmaktadır. H&M ve Zara gibi güçlü markalar alışveriş merkezlerinde yer alan mağazalarını azaltarak tüketicilerini Internet üzerinden satın almaya teşvik etmekte, Türkiye'de ise bunun öncülüğünü LCW ve Defacto gibi markalar yapmaktadır. Hatta Migros gibi zincirler gıda alışverişini Internet üzerine taşımaktadır. Medya alanında da değişimler yaşanmakta ve televizyon dizi ve filmleri geleneksel medya araçlarından koparak yeni medya aracı olarak nitelendirilen Internet televizyonları ve sosyal medyaları kullanmaya başlamışlardır. Gün geçtikçe Internet üzerinden alışverişin ve etkileşimin yaygınlaştığı ve daha da artacağı aşikârdır. Bu ürün ve hizmet satın alım esnasında ise kredi kartı ve kişisel bilgilerin kullanılması özellikle trojan ve benzeri programlarla bu bilgilerin ele geçirilmesinin önünü açmaktadır. Bu açıdan özellikle sanal kartların kullanımın arttırılması ve hatta kullanımının cazip hale getirilerek teşvik edilmesi, farkındalık yaratacak uygulamalara yer verilmesi ve bankaların elektronik ve mobil uygulamalarına girişlerinde daha önlem alıcı özelliklerin getirilmesi önem arz etmektedir. Tüketicilerin farkındalığı arttıkça, elektronik ticaret içerisine gireceği firmalardan daha güvenli bir hizmet sağlayıcısı beklentisi yaratılarak, firmaların da maksimum düzeyde önlem alması sağlanabilir. Ayrıca aynı bir aracı sigortalatır ya da kasko yaptırır gibi tüketicilerin kredi kartı ve banka kartı gibi sahip olduğu unsurlarını sigortalatmaları koşuluyla maddi kayıpların önüne geçilmesi de sağlanabilir.

Diğer bir önemli husus ise kötü amaçlı yazılımların siber tehdit oluşturmasıdır. Bilgisayarlara indirilen programlarla birlikte gelen kötü amaçlı yazılımlar kişilerden bağımsız hareket etmekte ve bir nevi siber ordu kurarak çeşitli saldırılar düzenlemektedir. Bu saldırılardan bilgisayar sahibinin çoğu zaman haberi olmamakta ve kendisi bir zombi bot olarak kullanılmaktadır. Ancak bilgisayarın karıştığı bu siber suçlar kişilerin de ceza almasına neden olabilmekte ve kişiler ya da kurumlar itibar ve de maddi kayıplarla karşı karşıya gelebilmektedir. Hackerların

bilgisayarlara ve tarayıcılara sızmasıyla önemli firmaların ve kurumların web sitelerinde değişiklik yapabildiği ve kamuoyuna yanlış bilgi verebildiği, hatta hakaret boyutuna varan paylaşımlara sebebiyet verdiği görülmüştür. Kurumsal itibar adına zedeleyici olan bu husus konusunda firmaların çalışanların bilgisayar güvenliğini sağlama ve kötü amaçlı yazılımları indirmesi önüne geçecek önlemler alma konusunda harekete geçmesi gerekmektedir. Ulaştırma bakanlığı siber tehdit ve siber güvenlik üzerine konferanslar düzenlemeye ve bu tehditleri ele almaya başlamıştır. Ancak bu konferansların yaygınlaştırılması, hatta bilgisayar ve Internet kullanımı yaşının düşmesi sebebiyle okullarda ders olarak verilmesi zararın en aza indirilmesi açısından önemlidir.

Türkiye'de siber güvenlik ve korsan ile savaşa yönelik alınan yasalar daha da ağırlaştırılarak ve denetimlerin arttırılmasıyla özellikle kötü amaçlı yazılımların kolay bir şekilde yayılmasına sebebiyet veren korsan yazılımların ediniminin önüne geçilmesi ve gerek bu programları hizmete sunan gerekse bilgisayarına indirme suretiyle haksız yere yararlanmaların en aza indirgenmesi gerekmektedir. Kamusal alanda da tüketicilerin e-devlet gibi uygulamaları kullandığı düşünülerek kişisel bilgilerin korunumu daha denetlenebilir ve kişilerin bu uygulamaları kullanmada daha bilinçli ve sorumlu hale getirilmesi şarttır. Ne yazık ki halen bir çok kişisel bilgisayarda, hatta kamu kurumlarında dahi tehditleri en aza indirgeyebilecek koruma programları etkin kullanılamamakta ve bu programlara masraf gözüyle bakılmaktadır. Kişilerde ve kurumlarda bilinç düzeyi ve sorumluluk alanı arttırılarak kişilerin ve kurumların koruma programına yönelimleri üst düzeye çıkarılabilir.

KAYNAKÇA

ABRAMS, V. K. (2018). The Global Media Intelligence Report. 10 Eylül 2019 tarihinde https://www.emarketer.com/content/global-media-intelligence-2018 adresinden ulaşıldı.

AKAMAI, (2017). Soti Security Financial Services Attack Economy Report 2019. 02 Eylül 2019 tarihinde https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-financial-services-attack-economy-report-2019.pdf adresinden ulaşıldı.

AKHILOMEN, J. (2013). Data Mining Application for Cyber Credit-Card Fraud Detection System. *Proceedings of the World Congress on Engineering*, 3, 1-6.

AL-KHATIB, A. M. (2012). Electronic Payment Fraud Detection Techniques. *World of Computer Science and Information Technology Journal*, 2(4), 137–141.

BAL, M. A. (2003), *Modern Devlet ve Güvenlik* (1. Baskı). İstanbul: IQ Yayınları.

BARIŞIK, S. ve TEMEL, H. (2007). İnternet Bankacılığı Kullanımında Güvenlik Unsurlarının Bilinilirliği (Anket Uygulamasına Dayalı SPSS Çözümlemesi). *Karamanoğlu Mehmetbey Üniversitesi Sosyal ve Ekonomik Araştırmalar Dergisi*, 2007(2), 136-160.

BAYRAKTAR, T. (20134). Karşılaştırmalı Sosyal Güvenlik Sistemleri: Türk Sosyal Güvenlik Sistemi Yapısı. *8-9 Ekim 2013 Ulusal Güvenlik Kongresi Bildiri Kitabı*, 1299-1309.

BAYRAKTAR, G. (2015). *Siber Savaş ve Ulusal Güvenlik Stratejisi*. İstanbul: Yeni Yüzyıl.

BİLGEN, M. (2009). Internet Bankacılığından Kaynaklanan Zararlarda Bankaların Sorumlulukları. *Bankacılar Dergisi*, 71, 78-97.

CAN, F. (2019). 06.08.2021 tarihinde https://tr.euronews.com/2019/12/11/siber-guvenlik-sirketi-turkiye-de-460-bin-kredi-kart-bilgisi-calind-karaborsada-sat-sa-sun adresinden ulaşıldı.

COHEN, F. (1987). Computer Viruses: Theory and Experiments. *Computer&Security*, 6, 22-35.

DARILICI, A. B. ve ÖZDAL, B. (2018). Analysis of the Cyber Security Strategies of People's Republic of China. *Güvenlik Stratejileri*, 14(28), 1-35.

DENNING, D. (2001). Is Cyber Terror Next?. 15 Nisan 2011 tarihinde http://essays.ssrc.org/sept11/essays/denning.htm adresinden ulaşıldı.

DHA, (2021). 06.08.2021 tarihinde https://www.ensonhaber.com/teknoloji/e-ticarete-yapilan-siber-saldirilar-artti-ilk-hedef-odeme-bilgileri adresinden ulaşıldı.

ENISA, (2016). Security of Mobile Payments and Digital Wallets. The European Union Agency for Network and Information Security. 02 Eylül 2019 tarihinde www.enisa.europa.eu/WP2016%203-1%204%20Mobile%20Payments%20Security.pdf adresinden ulaşıldı.

EPSTEIN, A. R. ve BROWN, P. T. (2008). Cybersecurity in the Payment Card Industry. *University of Chicago Law School Journal Articles*, 75 U. CHI. L. REV., 203-224.

ETİ, İ., G. ve ASLAN, B. (2008). İnternette Ödeme ve Güvenlik. *XIII. Türkiye'de İnternet Konferansı 22-23 Aralık 2008*, Ankara:Orta Doğu Teknik Üniversitesi, 113.

ETİCARET, (2021). İstatistikler, 11.03.2021 tarihinde https://www.eticaret.gov.tr/istatistikler adresinden ulaşıldı.

GONZÁLEZ, L. J. ve JOUANJEAN, M. (2017). Digital Trade: Developing a Framework for Analysis. *OECD Trade Policy Papers*, 205, 1-26.

GÖZTEPE, K., KILIÇ, R. ve KAYAALP, A. (2014). Cyber Defense In Depth: Designing Cyber Security Agency Organization For Turkey. *Journal of Naval Science and Engineering*, 10(1), 1-24.

JAIN, M. ve BAJAJ, P. (2014). Techniques in Detection and Analyzing Malware Executables: A Review. *International Journal of Computer Science and Mobile Computing*, 3(5), 930-935.

KARACI, A., AKYÜZ, H. İ. ve BİLGİCİ, G. (2017). Üniversite Öğrencilerinin Siber Güvenlik Davranışlarının İncelenmesi. *Kastamonu Eğitim Dergisi*, 25 (6), 2079-2094.

KOVACIK, M., KAJAN, M. ve ZADNIK, M. (2013). Detecting IP Spoofing by Modelling History of IP Address Entry Points. *Conference Paper: AIMS 2013*, Lecture Notes in Computer Science (7943), 1-11.

LEWIS, J. A. (2018). Economic Impact of Cybercrime. 02 Eylül 2019 tarihinde https://www.csis.org/analysis/economic-impact-cybercrime adresinden ulaşıldı.

MALWAREFIXES, (2019). PUP.Optional.InstallCore. 01 Eylül 2019 tarihinde https://malwarefixes.com/threats/pup-optional-installcore adresinden ulaşıldı.

MICROSOFT, (2019). Microsoft Security Inttelligence. 02 Eylül 2019 tarihinde https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=PUA:Win32/InstallCore adresinden ulaşıldı.

O'REIRDAN, M. (2011). Why Bother With Best Practices? Or Why Global Collaboration is Faster (and More Effective) Than a Speeding Bullet. *Cyber Security, New Europe (Special Edition)*, May-June 2011, 17.

ÖZMEN, Ş. (2013). *Ağ Ekonomisinde Yeni Ticaret Yolu: E-Ticaret*. İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

PIGNI, F., BARTOSIAK, M., PICCOLI, G. ve IVES, B. (2018). Targeting Target With A 100 Million Dollar Data Breach. *Journal of Information Technology Teaching Cases*, 8(1), 9–23.

RAY, I. ve POOLSAPPASIT, N. (2005). Using Attack Trees to Identify Malicious Attacks from Authorized Insiders. *Proceeding Book of Computer Security - ESORICS 2005*, 10th European Symposium on Research in Computer Security, 231-246.

RESMİ GAZETE, (2012). Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar. 01 Ağustos 2019 tarihinde http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf adresinden ulaşıldı.

RESMİ GAZETE, (2015). Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik. 02 Ağustos 2019 tarihinde http://www.resmigazete.gov.tr/eskiler/2015/07/20150715-4.htm adresinden ulaşıldı.

SCHULTZ, M. G., ESKIN, E., ZADOK, E. ve STOLFO, S. J. (2001). Data Mining Methods for Detection of New Malicious Executables. *Proceeding Book of Conference: Security and Privacy*, 38-50.

SİBERGÜVENLİKZİRVESİ, (2021). Siber Güvenlik Ekosisteminin Geliştirilmesi Zirvesi Sonuç Raporu. 10.02.2019 tarihinde https://www.siberguvenlikzirvesi.org.tr/2018/wp-content/uploads/2018/02/TBD-Siber-Guvenlik-Zirvesi-Sonuc-Raporu.pdf adresinden ulaşıldı.

SOHAIL, M. S. ve SHANMUGHAM, B. (2003). E-Banking And Customer Preferences İn Malaysia: An Empirical Investigation. *Information Science*, 1 (3-4), 207-217.

SOME (Siber Olaylara Müdahale Ekibi), (2019). Phishing Saldırıları ve Sahte Sistemler. 01 Eylül 2019 tarihinde https://some.nevsehir.edu.tr/tr/oltalama-phishing-e-postalari adresinden ulaşıldı.

THURAISINGHAM, B. (2005). *Managing Cyber Threats: Issues, Approaches, and Challenges*. Kumar, V., Srivastava, J. ve Lazarevic, A. (Ed.), Managing, Threats to Web Databases and Cyber Systems (3-19), USA:Springer.

TODAIE (Türkiye ve Orta Doğu Amme İdaresi Enstitüsü) (1992). *Kamu Yönetimi Araştırma (KAYA) Yerel Yönetimler Araştırma Grubu Raporu*. Ankara: TODAİE Yayını.

TUBİSAD (2017). Dtp Siber Güvenlik Raporu. 02 Eylül 2019 tarihinde http://www.tubisad.org.tr/tr/images/pdf/dtp_siber_guvenlik_raporu_4_0.pdf adresinden ulaşıldı.

UDHB (2016). 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı. 01 Eylül 2019 tarihinde http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf. adresinden ulaşıldı.

ÜNVER, M. ve CANBAY, C. (2015). Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik. *Elektrik Mühendisliği*, 438, 94-103.