KSÜ Mühendislik Bilimleri Dergisi, 27(4), 2024
Araştırma Makalesi

KSU J Eng Sci, 27(4), 2024
Research Article

Kahramanmaras Sutcu Imam University
Journal of Engineering Sciences

Geliş Tarihi : 02.05.2024
Kabul Tarihi : 22.07.2024

Received Date : 02.05.2024
Accepted Date : 22.07.2024

SİBERUZAMDA SUÇ TİPOLOJİLERİ VE SİBER İLETİŞİM TABANLI ÇÖZÜMLEME MODELİNİN ANALİZİ

TYPOLOGIES OF CRIME IN CYBER SPACE AND ANALYSIS OF CYBER COMMUNICATION BASED ANALYSIS MODEL

Mustafa AYDEMİR[1] (ORCID: 0000-0001-9414-4053)

[1]Ege Üniversitesi, Uluslararası Bilgisayar Enstitüsü, İzmir, Türkiye

*Sorumlu Yazar / Corresponding Author: Mustafa AYDEMİR, dr.mustafa.aydemir@gmail.com

ÖZET

İnternet tabanlı ağ teknolojilerinin hızlı dönüşümü, bireylerin sanal ortamlarda gösterdikleri katılımı günden güne artırmaktadır. İnternet ortamı diğer kişilerin verilerini illegal olarak elde etmeyi hedefleyen kişiler tarafından da yoğun olarak kullanılmaktadır. Siber dünyada kazanma davranışı ve korsanlık sorunsalı fiziksel alanlardan dijital alanlara doğru geçiş yapmaktadır. Bu çalışmada, siber uzamda yapılan yasadışı işlemlere karşı getirilen özelleştirilmiş Alan Adı Sistemi üzerinden sorgu takipleri yapılmıştır. Uygulama sürecinde, bir aylık tam ölçümlü ve kesinlikli veri akışları dizgesi ile sorgu ve diğer analizlerin takibi yapılmıştır. İçerik analizi kapsamında uygulama üzerinden yapılan izlemede, 64 toplam filtreleme listesi içinde 48 adet yabancı filtre (%87,3) Türk filtre olarak 7 adet (%12,7), ve 9 adet ortak filtre tipolojisi özelliği gösteren filtreler ortaya çıkmaktadır. Sorgulama konusunda; dört temel değer sistemi oluşturularak Alan Adı Sistemi Sorgu Sayısı, Engel Sayısı, Kötü Amaçlı Yazılım ve Kimlik Avı ile Yetişkin İçerikli Siteler şeklinde sistem oluşturulmuştur. Çalışmada, ilgili yönerge üzerinden IP ve Alan Adı Sistemi örnekleri üzerinden suç tipolojilerinin düzeyleri istatistiksel olarak analiz edilmektedir.

Anahtar Kelimeler: Siber suç, siber uzam, filtreleme, alan adı sistemi, içerik analizi

ABSTRACT

The rapid transformation of Internet-based network technologies increases the participation of individuals in virtual environments day by day. The internet environment is also used extensively by individuals who aim to illegally obtain other people's data. In the cyber world, the problematic of acquisition behavior and piracy is shifting from physical to digital spaces. In this study, query monitoring was carried out through the customized Domain Name System introduced against illegal transactions in cyberspace. During the implementation process, queries and other analyses were tracked using a one-month set of fully measured and precise data streams. Follow content primarily conducted through the application specified in the scope of the analysis for filtering, filtering in the list according to the analysis of a total of 64, 48 foreign filter (%87,3) Turkish as a filter 7 units (%12,7), and 9 common feature filters which filter typology emerges. Regarding the query; four basic value systems have been created and the system has been created in the form of the Number of Domain Name System Queries, the Number of Obstacles, Malware and Phishing, and Adult Content Sites. In the study, the levels of crime typologies are statistically analyzed through IP and DNS samples over the relevant directive.

Keywords: Cybercrime, cyberspace, filtering, dns, content analysis

ToCite: AYDEMİR, M., (2024). SİBERUZAMDA SUÇ TİPOLOJİLERİ VE SİBER İLETİŞİM TABANLI ÇÖZÜMLEME MODELİNİN ANALİZİ. *Kahramanmaraş Sütçü İmam Üniversitesi Mühendislik Bilimleri Dergisi*, 27(4), 1375-1400.

GİRİŞ

Bilgi ve iletişim teknolojilerinin ağ üzerinden biçimlendiği yeni yüzyılda kullanıcıların ağ hareketlerinin sanal düzlemde kimlik kazanmasıyla web tabanlı dijital eğilimler önem kazanmaya başlamıştır. Web teknolojilerinin yapay zekayla olan etkileşimli yapısı dijital alanın tasarım modellerini değiştirmektedir. Sanal sistemlerin kullanıcılar üzerinde ağ kimliğini belirleyen deneyimleme modeli, yeni medya düzeninin internet uzantısını oluşturmaktadır. Sanal kimliğin sınırlarının internet üzerinden sınırsızlık halini alması, kuralsızlaşma ve hakimiyet yitimi gibi bazı negatif görüşlerin de etkinlik kazanmasına neden olmaktadır. Zira sınırsız bir sanal evren tasarımının web alanı üzerinden gerçekleşmesiyle yasadışı işlemlerde yaşanan artış suç ve ceza kavramlarını sorgulanır hale getirmektedir. İnternet, kullanıcının deneyimleme alanı olarak, suç ve şiddet gibi zarar etkisi oluşturan dijital bir ortamın da betimlemesi dahilindedir.

İnternet içerikleri ve içeriklere yönelik ortaya çıkan "virüs, siber saldırı, sanal dolandırıcılık, haksız kazanç elde etme ve sosyal mühendislik gibi" yönelimler, sanal ortamda kaos yaratmaktadır. Bu noktada, kaosun çözümü için ilgili platform ve hizmet sağlayıcılarının kurumsal (ticari ve kamu kaynaklı) ve kişisel (bireysel kullanıcı) çözümlemeler ile muhtemel siber zararlara karşı koruyucu politikalar oluşturulmaktadır. Siber güvenlik, ağ oluşturma ve programlama teknolojileri kullanarak tüm cihazları ve verileri dışarıdan gelebilecek siber saldırılara karşı kontrol etme uygulamasıdır. Siber güvenliğin temel amacı, siber saldırılarla ilgili tüm riskleri azaltmanın yanı sıra iş sistemi teknolojisinin ve ağların yetkili kullanımına karşı koruma sağlamaktır (Lippert ve Cloutier, 2021; Rass vd., 2020; Fielder vd., 2018).

Siber alanda öz varlığını temel altyapı ve satın alma konusundaki önemli ekonomik yatırımlar ile güvence altına almaya çalışan kurumlar karşısında bireysel kullanıcıların kendini ve ailesini muhtemel problemlere karşı korumak üzere sorumluk ve inisiyatif alma düzeyleri değişmektedir. Günümüzde söz konusu siber saldırıların önlenmesi konusunda tespit edilme konusunda özellikle "veri paylaşım modeli ve tehdit avcılığı" (Yetimoğlu, 2022) gibi çeşitli çalışmalar yapılmaktadır. İnternet tabanlı uygulamaların kurulum ve kullanma süreçlerinde yaşanan veri ihlallerini engellemek üzere erişim ve güvenlik konularında çeşitli yöntemler kullanmaktadır. Sanal dünyada ağ kullanıcılarının iletişim bilgilerinin yanı sıra çift doğrulama gibi çeşitli güvenlik onayları zorunlu tutulabilmektedir. Bu politikalar, ağ kullanıcıları üzerinde veri güvenliği ile siber denetim konularında bilinçli olması konusunun önemli olduğuna dikkat çekmektedir. Zira kullanıcıların yaş, cinsiyet ve diğer kimlik bilgilerinin internet tabanlı mecralarda arşivlenmesi dışında veri analiz şirketlerince pazarlanması veri güvenliğini tehditlere açık duruma getirmektedir. Kimliğin sanal dünyada kontrollü yayılımına ek olarak siber saldırılarla yasadışı amaçlarla kullanılması, ağ yönelimi konusunda bireylere önleyici sistemler kullanmaları için alternatif yol arayışına yönlendirmektedir. Ağ üzerinde kullanım ve dijital adımlarının tespit edilmesi için yapılan saldırılar karşısında koruyucu program ve bir dizi denetim çabaları sonucunda güvenli internet alanı yaratılmaktadır. Siber uzam, sanal dünyada tüm ağ trafiklerinin kapladığı sanal bütünlüğü sağlamış yapıyı ifade etmektedir. Bireylerin küresel medya sistemi içinde kendini ifade edebilmesinin en kolay ve hedef odaklı hali, sanal dünyada açtığı hesaplar ve bu hesaplardaki ağ hareketlerinin düzeyi ile ilişkilidir.

Günümüz medya ve iletişim teknolojileri dış etkilere açık bir yapıdadır. Bireylerin ve kurumların açtıkları hesaplar, içerik yapıları ve veritabanı gibi hassas alanları içerdiğinden düzenli bir saldırı ve tehdit altındadır. Son yıllarda sanal hesaplar (e-posta, sosyal medya hesapları, web tabanlı hesaplar, banka hesapları vb.) diğer kullanıcılar tarafından siber saldırılarla ele geçirme çabaları karşısında koruma, yüksek güvenlikli çözümler ve önleyici koruma politikalarıyla desteklenmektedir. Bu noktada kişisel ya da kurumsal nitelikli hesaplara ulaşmak, bu hesapların sahte biçimlerini üreterek, ilgili hesapların kullanıcı adı ve şifrelerine erişmek sıklıkla karşılaşılan yasadışı çalışmalardır. Yine ilgili hesap veya bir sistem üzerinden veri tabanını yasadışı yollarla yedeklemek ve diğer kullanıcılara satışını yapmak gibi sızma eylemleri karşısında kullanıcıların çözümler üretmesi gerekmektedir. Kullanıcılar kendi medyaları ile hesaplarını düzenli taramak, güncel şifreleme sistemlerinde değişiklik yapmek ve en güncel riskleri takip ederek etkin çözümler üretmekle yükümlüdür. Zira kullanıcıların sistem ya da medya ağının da daha yüksek ölçekte siber saldırıya uğraması ve büyük ölçeklerde zarar görmesi olasıdır. Yeni medya düzeninde sanal ortamlarda ön plana çıkmak ve imaj üretmek için yapılan saldırılar dışında ekonomik kazanç elde etmek, sosyal mühendislik yapmak, istihbarat faaliyetlerini gerçekleştirmek gibi geniş bir yelpazede siber saldırılar yapılmaktadır. Bu davranışlara ek olarak rakip ya da düşman görülen ticari rekabet halindeki diğer hesaplara zarar verip kurumsal imajını zedeleyerek potansiyel müşteri tarafgirliği oluşturmak, stratejik planlamalarla rakiplerin ticari faaliyetlerini geçici de olsa erteletebilmek üzere yapılan tüm işlemler yapısal benzerlikle birlikte suç açısından farklı tipolojik özellikleri göstermektedir.

Sanal dünya, bireylere sanal bir kimlik oluşturarak eylemlerini gerçekleştirme, diğer kullanıcılarla etkileşimli bir bağ oluşturma, günlük yaşam pratiklerini içeren satın alma, bankacılık, diğer kullanıcıların günlük deneyimlerini takip etme, gündemi yakalama ve kendi içeriğini oluşturma gibi katkılar sağlayabilmektedir. Bu katkılar, bireysel olduğu gibi kurumsal ve ticari bazlı gerçekleşebilmektedir. Sanal hesapların yönetimi ve denetimi ise bu haber akışının sağlanması, verilerin çalınmaması ve diğer kullanıcılara (arkadaş listesi, müşteri listesi gibi) ait özel bilgileri içeren enformasyon alanlarına dair veri güvenliği politikalarının da tasarlanmasını zorunlu hale getirmektedir. Bireysel kullanıcılar kendi güvenlik önlemlerini geliştirmek adına daha önce ifade ettiğimiz önlemlerin yanı sıra değişen teknolojilere bağlı olarak düzenli şifre değiştirmek ya da antivirüs programı kurmak dışında gerek mobil gerekse masaüstü çözümler de üretmeyi düşünebilmektedir. Kurumsal ve ticari düzeyde daha yüksek veri işleyen kuruluşlar ise müşteri ya da takipçi listelerinin veri güvenliğini sağlamak ve sızma girişimlerini engellemek için karmaşık bir uygulama yönergesi uygulamakla yükümlüdür. Bu noktada kaynağı belirsiz içerikler karşısında antivirüs çözümlerini yeterli görmeyip, alanında uzman siber güvenlik personelini istihdam etmek; web site, kullanıcı hesapları, sosyal medya hesapları ve sanal sunucu güvenliği gibi alanlarda önleyici güvenlik niteliğine sahip koruma politikaları hazırlamak önemli bir husus olarak karşımıza çıkmaktadır.

Bu çalışmada, kuruma özel hedef gözeten saldırıların hızlı bir şekilde bertaraf edilmesi sağlanmaktadır. Bu sayede ilgili kuruma ait bir veritabanı oluşturulmasını sağlamak üzere merkezi olarak izleme ve müdahaleyi kolaylaştıran bir arayüz tasarlanmaktadır. Bu arayüz sayesinde birden fazla yönetimsel ekranı izlemek, güvenlik kuralı oluşturmak ve dağıtık olarak inşa edilen diğer güvenlik sistemlerinin yerine tümleşik ve merkezi bir izlemenin nasıl yapılabileceği örnek bir uygulama üzerinden sunulmaktadır. Çalışmanın bu bağlamda önemi günümüz koşullarında çok çeşitli yazılım ve sistemler tarafından üretilen çıktıların tek bir arayüz üzerinden analiz edilerek zaman ve personel kaynağının önüne geçilmesi konusunda örnek bir çalışma modelini ortaya koymasıdır. Söz konusu çalışmanın uygulama modeli, kuruma özel güvenlik sistemlerinin kaynak tipolojileri ve önlem biçimlerini merkezi olarak nasıl yönetilebileceğini göstermesi noktasında referans olarak önemli bir boşluğu doldurmaktadır.

LİTERATÜR TARAMASI

Çalışma kapsamında siber uzam, siber suç, güvenli internet, siber aylaklık, siber psikoloji ve dijitalleşme, yapılan literatür taramasında ön plana çıkan kavramlar arasındadır. Siber uzam; sanal dünya, internet dünyası, telekomünikasyon temelli ağ sistemi ve dijital varlık alanını temsil etmektedir. Siber uzam kavramı, ilk kez William Ford Gibson tarafından bilim kurgu eseri olan Neuromancer adlı romanda kullanılmıştır (Gibson, 1984). Medin (2018), internetin değiştirici ve dönüştürücü özelliğini siber uzam konusunun yeni bir kamusal alanı olarak düşünüldüğünü belirtmektedir. Toplumsal ilişkilerin sanal bağlar-ağlar üzerinden yürümesi (Zinderen, 2020) şeklinde ifade edilen siber uzam alanı, bireylerin özne ve nesne olma noktasında sanal kimlik kazanma süreçlerindeki dönüşümünü hızlandırmaktadır. Siber uzam, "bilgisayar ağlarının birbirine bağlanması sonucu ortaya çıkan makine-insan ilişkisi temelindeki dönüşümü" ifade etmektedir (Stratton, 2002, s.80). Siberuzam kavramı "elektronların ve elektromanyetik spektrumun birlikte kullanımıyla karakterize edilen, amacı bilgi yaratmak, depolamak, değiştirmek, değiş tokuş etmek, paylaşmak ve çıkarmak, kullanmak, ortadan kaldırmak ve fiziksel kaynakları bozmak olan küresel ve dinamik bir alan olarak tanımlanmaktadır (Kuehl, 2009, s.26-28). Siber uzam konusu ayrıca zaman ve mekândan bağımsız olma, farklı mekanlar arası geçiş sağlama ve internet tabanlı temsillerin gerçekleştiği bir yapıyı ifade etmektedir. Timisi ise siber uzamı "elektronik olarak dolayımlanmış ya da benzeşmiş bir uzamda karşılaşma olanakları olan gerçek ya da hayali ilişkiler" şeklinde tanımlamaktadır (2005, s.91). Siber uzam alanı yapay zekâ ve diğer gelişmelerin de etkisiyle son dönemlerde sosyal ağlarda görüldüğü üzere kişilik özellikleri ve kimliği de şekillendirmektedir.

Nagy ve Koles, siber uzamda yeni gelişmelerin gerçek dünyada gösterilemeyen özelliklerin avatarlar üzerinden sanal gerçekliğe dönüştürülebildiğini (2014, s.4) belirtmektedir. Bauman ve Lyon (2013) ise gözetim konusunun, siber uzam aracılığıyla elde edildiğinden hareketle dolaysız bir biçimde kullanılabildiğini ifade etmektedir. Bu örnekler ışığında siber uzam konusu bireylerin bedenleri yerine sanal kimlikleri üzerine inşa ettikleri ve ilgili internet altyapısı ve erişim sağladıkları diğer sosyal ağlar üzerinden yarattıkları dijital eylemlerin toplamına karşılık gelmektedir. Turkle (1996) ise otantik ve çoklu bir kimliğin inşa edilmesini olanaklı hale getirmesi açısından siber uzam alanının fırsat yaratabileceğini belirtmektedir. Kimliğin sanal ortamda bedensizleşmesi ya da sanal bedene ve mekanlara dönüşmesi ise siborg, sibernetik ve siber tektonik (Clynes ve Kline, 1960; Akman, 1982; Cutler, 1996; Shusterman, 2000; Haraway, 2006; Kut, 2013) kavramlarıyla temellendirilmektedir. İnsan bedeninin beyin ile makine (bilgisayar temelli) ekseninde oluşturduğu bu yeni form, bedenin fiziksel özelliklerinin sınırlandırılarak ya da organizma özelliklerinin genetik düzeninin elektronik bağlamda değişebileceğini ve böylece siber uzamda beden

yönetimi ve sanal hakimiyetin yeni forma göre düzenleneceğini açıklamaktadır. Siber uzam alanını sosyolojik açıdan değerlendiren ve tipolojilere ayıran Bağrıyanık, (2018) çalışmasında "dijital insan, trol, youtuber ve oyuncu" olmak üzere dört temel formda tipoloji olduğunu belirtmektedir. İnsanın, dijital alanda kültürlenmesi ve kendisi dijital kültürün bir ögesi olarak kimlikten e-kimliğe, insandan e-insana ve diğer alanlarda da "e-leşme" süreci, dijital toplumdaki bireyin siber uzamdaki karşılığını tanımlamaktadır.

Siber Suç, dijitalleşmeyle birlikte ağ toplumunun nesnesine dönüşen bireylerin sanallaşma çabaları bazı riskleri beraberinde getirmektedir. Siber ortamda farklı ağ hesaplarına erişim sağlayan ya da içeriklere yönelen bireylerin kendilerinin yasal sınırda kalıp kalmaması kadar muhtemel siber saldırılar karşısında suç eyleminin mağduru olması ihtimali de bulunmaktadır. Siber suç konusunu inceleyen araştırmalar; Yapay içeriklerin gerçeğin yerine geçmesi (Metin ve Karakaya, 2017), siber zorbalık (Li, 2006; Erdur-Baker ve Kavşut, 2007; Arıcak vd., 2008; Hinduja ve Patchin, 2009; Smith, 2011; Bulut ve Gündüz, 2012; Kowalski vd., 2012; Yaman ve Peker, 2012; Cassidy vd., 2013; Kowalski vd, 2014; Peker ve Ekinci, 2016; Akyüz ve Koç, 2020; İşman ve Açmacı, 2021), Siber Mahremiyet (Simpson ve Murphy, 2014; Do vd., 2017; Wang, 2019), Zararlı İçerik Gönderisi (Bargh ve McKenna 2004; Willard, 2004; Greene, 2006; Lacey, 2007; Lenhart, 2007; Wong-Lo ve Bullock, 2011), Siber Saldırı (Slonje ve Smith, 2008) gibi türlerden oluşmaktadır. Siber suç, bireyin sanal içeriği elde etme ve içeriği yorumlama biçimi, eleştirel söylemlerini paylaşımlarla suça dönüştürme, internet ve bağlı alanları, diğer hesapları ele geçirme, mobil tabanlı saldırılar, siber müdahalede bulunma gibi alanlarla bağlantılı olarak ortaya çıkmaktadır.

Güvenli internet, sanal ortamlarda siber uzamın gelişimi sonucu ortaya çıkan sorunların çözüm amaçlı kavramıdır. Günümüzde bilgi ve iletişim teknolojilerinin kuşatıcı etkisiyle bireylerin kendilerini suç ve diğer olası tehditler karşısında korumaya alabilmesi için antivirüs programlarının yanı sıra filtreleme çalışmaları, yazılımsal düzeyde diğer alternatif uygulamalar arasındadır. İnternet mecrasını, eğitim ve öğretim faaliyetleri kapsamında kullanımının yoğunlaştığı pandemi sürecinde özellikle siber zorbalık, şiddet, bağımlılık ve intihar gibi sosyo- psikolojik sorunlar karşısında kullanıcıların güvenli internet alanına duydukları ihtiyacı artırmaktadır. Güvenli internet konusunu ele alan çalışmalar arasında Schroeder, 2002; Korkmaz ve Kıran-Esen, 2012; Kaşıkçı vd., 2014; Aslan ve Karakuş Yılmaz, 2017; Tuparova ve Mehandzhiyska, 2018; Abide ve Gelişli, 2020; Akgün, 2022) yer almaktadır. Bu çalışmalar temel olarak internetin zararlarını en aza indirebilmenin yollarını arasa da yapılan saha araştırmalarıyla internetin olası etkileri, zararları ve baskın yönlerini değerlendirmektedir. Güvenli internet alanı temelde siber güvenlik, (Pusey ve Sadera, 2012; Van Schaik, 2017), siber etik (Brown ve Wang, 2008), siber koruma (Nowicki, 2002) ve sağlıklı internet (Çetin ve Ceyhan, 2014) kavramlarıyla ilişkilendirilmektedir.

Yine ilgili araştırmalarda özellikle öğrenci ve ebeveynlerin bu alanda yaşadıkları olumsuz olaylar karşısında çözüm yolları ve genel tepkileri de incelenmektedir. Güvenli internet, esas itibariyle, içeriğin özelliği, diğer kullanıcıların doğrudan ya da dolaylı etkileri ile akran zorbalığı, tehdit ve şantaj gibi değişen dolandırıcılık yöntemlerinin de etkisiyle güvensiz bir dijital platforma dönüşen internet alanı ile mobil tabanlı sistemlerin içinde yer alan uygulamalar ve sosyal ağların verebileceği zararlar karşısında bireylerin değişen tercihlerini ifade etmektedir.

Siber Aylaklık kavramı literatürde temel olarak "cyberloafing" ve "cyberslacking" şeklinde kullanılmaktadır. Bu alanda ayrıca siber tembellik, kaytarmacılık şeklinde kullanımlar da yer almaktadır. Siber aylaklık konusunda genel olarak iş motivasyonu, süreç yönetimi, eğitim, zaman kaybı gibi araştırmalar (Lim, 2002; Ugrin.,vd 2007; Blanchard ve Henle 2008; Garrett ve Danziger, 2008; Yağcı ve Yüceler, 2016; Yazgan ve Yıldırım, 2020; Beugre ve Kim, 2006; Kalaycı, 2010; Vitak, vd., 2011; Lim, 2012; Ergün ve Altun, 2012; Yaşar ve Yurdugül, 2013; Akbulut vd., 2016; Arabacı, 2017; Alan, 2019; Şenel vd., 2019) yanında sanal rahatlama ve deneyim gibi konuları ele alan (Anandarajan ve Simmers, 2005) çalışmalar da bulunmaktadır. Siber aylaklık özellikle zaman yönetimi konusunda bireylerin mobil cihazlarda ya da kişisel ve dizüstü tabanlı bilgisayar gibi teknolojik araçlarda yapılması gereken iş yönetimleri konusunda, iş planlarında yaşadıkları aksaklık ya da plansızlık gibi bir işi bırakıp diğer işe yönelerek nitelikli süreç yürütülmemesidir. Bir işlemin sonlandırılmaması ya da geç tamamlanması niteliksiz zaman ve olası masraf artışına da neden olduğundan süreç yönetimi konusunda kaygı ve isteksizlik halinin ortadan kaldırılması için siber dünyada iş eylemlerinde planlama yapılmasının tüm dijital aktivitelerde deneyimleme konusunda aylaklık algısını değiştirileceği kabul edilmektedir.

Siber psikoloji, McLuhan'ın (1964) vurguladığı haliyle insanın yeni bir uzantısı olma hali, süreç içinde kimliği ve kişiliğinin uzantısına; psikolojik (Suler,1996) temelli, bilişsel ve iletişimsel özelliklere de dönüşebilmektedir. Siber alan içinde bireyin sanal kimliği ve hesap hareketleri etkileşim halindedir. Kullanıcının gerçek kimliği ve kişiliği sanal dünyada birebir örtüşmek ya da uyumlu olmak zorunda olmadığı gibi sınırlandırmama konusundaki ruh hali;

Sayar'ın "dezinhibisyon etkisi" (2002) olarak tanımladığı yüz yüze iletişim yerine sanal ortamda hareket kısıtlılığını psikolojik bir avantaja dönüştürmesi durumu siber psikoloji alanını tanımlamaktadır. Krueger, sanal ortamda inşa edilen karakterin fiziksel özellikleri ya da görünümünün ne olduğunun önemli olmadığı yapay gerçeklik ile bunun bile üzerinde oynanabileceğini ileri sürmektedir (1991). Bu açıdan sanal ortamda inşa edilen gerçeklik ile bireyin kendi gerçekliği bir izlenim yönetimine (Tedeschi vd., 1985; Becker ve Martin, 1995; Bozeman ve Kocmar, 1997; Ralston ve Kirkwood, 1999; Martin ve Leary, 1999; Özdemir, 2006) dönüştüğünden algı yapısı ve uyumluluk konusundaki psikolojik eşik sanal dünyadaki davranış setleri ve engellenmişlik durumu ile ilişkilendirilmektedir.

Dijitalleşme, dijital ve sanal teknolojiler tarafından çerçevelenmiş ağ toplumu özelliğine dönüşen yapıları ifade etmek için kullanılmaktadır. Dijital olma, yenilikçi, etkileşimli, yakınsak ve küresel medya telekomünikasyon sistemleriyle uyumlu olma davranışlarını ve altyapıları temellendirmektedir. Dijitalleşmenin doğal bir karşılığı olan (Levy, 1997; Castells, 2005; Törenli, 2005; Öztürk, 2013) dijital alan hakimiyeti, bireyin üstünlüğü gibi görülmekle birlikte tüm medyalar arasılık ve yöndeşme yapısıyla kullanıcıların dijital bağlanma ve sanal karakter inşa süreçlerinde birbirinden farklı kullanıcı ve hesap tipolojileri oluşturabilmektedir. Tek ortamda tüm medyaların sarmal, iç içe geçme hali günümüz dijitalleşme süreçlerinde dijital alanlar ile kullanıcıların iletişim ve etkileşim düzeylerinde değişimler yaratabilmektedir. Dijitalleşme, tek tipli değildir. Kullanıcıların fizyolojik, psikolojik ve bilişsel süreçleri olarak içsel yeterlilikleri; teknoloji, çevre ve eğitim olarak dışsal yeterlilikleri ifade etmektedir. Dijitalleşme konusu, tarihsel süreçte görece daha iyi ve modern olanın seçimlenmesi olduğu kadar dijital alanların kuşaklar arası geçirgenliği ve aktarım sistemleriyle de ilişkisi bulunmaktadır.

SANAL SUÇ TİPOLOJİLERİ

Günümüz koşullarında gerçek hayatta gerçekleşen suç tanımlarının hemen hemen hepsi sanal dünya içerisinde de karşımıza çıkabilmektedir. İlgili suçlar kapsamında siber zorbalık, aldatma, çalma sıralanabilmektedir. Bu nedenledir ki tüm dünyada internet kullanımının ve güvenlik politikalarının hızla uygulanmasına geçilmiştir. Türkiye'de, Ulusal Siber Olaylara Müdahale Birimi (USOM), 5651 sayılı internet suçlarını kapsayan kanun ile 6698 sayılı kanun Kişisel Verilerin korunması kanunu (KVKK) siber suçlarla mücadele amacıyla oluşturulan güvenlik uygulamalarıdır. Bu bağlamda suç tipolojileri listesi[1] sıralanmaktadır.

İstenmeyen e-posta (Spam)

E-posta sahteciliği, insanların herhangi bir web sitesine kaydolurken kullanmış oldukları e-posta adreslerinin kişi rızası dışında toplanıp rahatsız edici boyutta reklam amaçlı olarak kullanılmasıdır. Reklamların içerikleri genelde yetişkin içerikli ürün, ilaç gibi reklam yasağı olan ürünlerin tanıtımı amacıyla kullanılmaktadır. İnternet ortamında yasal olmayan içerikleri oluşturmak ve bunları e-posta ve paylaşım gibi formüllerde yayılması resmi olarak ilk kez iki avukatın davayı kendi lehlerine çevirmek üzere spam mail göndermeleriyle ortaya çıkmıştır.

Spam kavramından ilk kez 31 Mart 1993'te bahseden Joel Furr, Canter ve Siegel'in spam gönderme çabaları karşısında "Yeşil Kart Avukatları: Dünyayı Spamlamak" yazılı tişörtler satmaya başlamıştır (Öztürk, 2013). Spam saldırıları bir yönüyle kendi reklamını yapmak, diğer kişiyi ve ürünlerini kötülemek gibi rekabet temelli içerikler üzerinden inşa edilebilmektedir. İnceleme spam'leri şeklinde tanımlanan bu eylemler, (TIFO, 2012) makine öğrenimi algoritmalarına dayalı inceleme spam tanımlama bileşenini incelemektedir. Sosyal medya araçlarının kullanımında siber suç konusunu oluşturan spam saldırıların bot olarak kullanımında makine öğrenmesi gibi çeşitli tekniklerle işlenmesinin önemli bir yönü olduğunu belirten Wang, (Li, vd. 2011) konuyu twitter platformu üzerinden ele alırken; Spam gönderenlerin, kötü niyetli bağlantılar içeren çok sayıda yinelenen güncellemeler ile kullanıcılara istenmeyen mesajlar göndermek, yanıtlama işlevini kötüye kullanmak ve trend olan konuları ele geçirmek için bir araç olarak kullandığını belirtmektedir.

Spam konusu tarihsel olarak; e-posta (Wang, 2010) Web (Gyöngyi vd., 2004; Bhowmick ve Hazarika, 2018) bağlamlarında incelenmiştir. Son zamanlarda araştırmacılar fikir spamlerini de incelemeye başlamıştır Raad vd.,2010; Jindal ve Liu, 2008; Wu, 2010). Jindal ve Liu (2008) fikir spamlerinin hem yaygın hem de doğası gereği e-posta ya da Web spamlerinden farklı olduğunu bulmuştur. Buna göre web spam'i iki ana türe ayrılabilir: İçerik spam'i ve bağlantı spam'i. Bağlantı spam'i, incelemelerde bulunmayan köprüler üzerinde yapılan spam'dir, çünkü incelemeler arasında genellikle bağlantı yoktur. İçerik spam'i, arama motorlarını hedef sayfaları üst sıralara

[1] Siber uzamda gerçekleşen siber saldırılara ait suç tipolojilerinin bilinirlik taşıyan küresel isimleri parantez içerisinde İngilizce olarak yazılmaktadır.

çıkarmak için kandırmak amacıyla hedef sayfalara alakasız veya uzaktan alakalı kelimeler eklemeye çalışmaktadır (Androutsopoulos vd., 2000). Söz konusu çalışmalar ağırlıklı olarak e-posta spam tespiti ve Web spam tespiti üzerine odaklanmaktadır (Yoo ve Gretzel, 2009). Spam e-postaları filtrelemek için Bayesci bir yaklaşımı ilk kez uygulamışlardır. Deney sonuçları, sınıflandırıcının e-posta mesajlarının ham metnine ek olarak alana özgü özellikleri de dikkate alarak daha iyi bir performans elde ettiğini göstermektedir.

Makine öğrenimi yardımıyla anti-spam filtreleme konusu önemli hale gelmektedir. Manuel spam veya spam olmayan olarak sınıflandırılmış mesajlar üzerinde eğitim aldıktan sonra spam e-postayı tanımlamayı öğrenen denetimli öğrenme yöntemlerini incelemektedir. Sahami vd., (1998) tarafından anti-spam filtreleme için bir Bayesci bir model üzerinden analizler yaparken, eğitilmiş ve görünmeyen mesajlar üzerinde etkileyici bir performans (Duda ve Hart,1973; Mitchell,1997), analizleri de yapılmıştır. Spam göndericileri yasadışı veya yasal olduğunu söyledikleri yollardan yaptıkları anlaşmalar üzerinden gönderim hizmeti yapmaktadır. İçeriği görüntülemeyle elde edilen gelir ile tıklama başına kazanılan ödeme, spam uygulamasının önemli çıktıları arasında yer almaktadır. Ayrıca e-postaların gönderimi için kullanılacak sunucu ve bilgisayarların kanuni yolla tespit edilip yasal işlem yapılması ihtimaline karşın diğer suçlarla ilişkili kullanılması da söz konusudur.

Kimlik Avı (Phishing)

Bu suç tipolojisi, Türkçe literatüre oltalama saldırısı veya kimlik avı olarak adlandırılan saldırı yöntemi şeklinde girmiştir. Oltalama, "tüketicilerin kişisel kimlik verilerini ve finansal hesap kimlik bilgilerini çalmak için hem sosyal mühendislik hem de teknik hile kullanan bir suç mekanizmasıdır" (Baykara ve Gürel, 2018; Bhavsar vd., 2018).1996'da ortaya atılan bir terim olan oltalama, ilk olarak AOL şifrelerinin ve ilgili hesapların çalınmasını tanımlamak için kullanılmıştır (APWG, 2013). İnsanların internete olan bağımlılığı arttıkça, bilgisayar korsanlığı, saldırı ve diğer güvenlik ihlalleri olasılığı da hızla artmaktadır (Clayton, 2005). Kişisel bilgisayar kullanıcıları, internet teknolojisinin hızlı büyümesi nedeniyle oltalama saldırılarına karşı hassastır Liang ve Xue, 2009; Purkait, 2012). Bireysel kullanıcıları oltalama tehditlerine karşı korumak için oltalama eğitiminin dikkate alınması gerekmektedir (Brody vd., 2007).

Oltalama konusunun engellenmesi konusunu ele alan araştırmalarda; Makine öğrenme tabanlı çözümlemeler (Allen, 2006), istatistiksel sınıflandırıcıları (Fette vd., 2007; Bergholz vd., 2010), E-posta içeriğinin kişiselleştirilmesi, aciliyet derecesi ve e-posta yükü, düşük teknik uzmanlığın yanı sıra duyarlılığın artmasına da katkıda bulunmak üzere çeşitli öneri modelleri geliştirilmektedir. Vishwanath vd., (2011) gibi araştırmacılar özellikle bu saldırılara karşı bilinçli olma ve savunma politikalarının önemine dikkat çekmektedir. Moore ve Clayton'a göre, kimlik avına karşı ilk savunma hattı otomatik tespit olmalıdır. Otomatik kimlik avı tespit yazılımları birkaç farklı seviyede mevcuttur: posta sunucuları ve istemcileri, internet servis sağlayıcıları ve web tarayıcı araçları. Araçlar tespit edilen kimlik avı web sitesine erişimi engelleyebilir ve/veya web sitesinin internet servis sağlayıcısından web sitesini kapatmasını talep edebilmektedir (2007). Oltalama konusunda bazı araştırmacılar (Arachchilage ve Love, 2013) kimlik avı saldırılarını engelleme motivasyonu yoluyla kullanıcı kaçınma davranışını geliştirmek için bir oyun tasarım çerçevesinin geliştirilmesi konusu ele almışlardır. Günümüz koşullarında gönderilen e-posta ekinde enfekte edilmiş pdf dokümanı ile gerçekçi görünen bir saldırı ile kullanıcı kandırılmaktadır ve bu sayede kullanıcıya ait veriler saldırganlara sunucu yoluyla iletilmektedir. Bunu engellemek üzere geliştirilen kişisel ve kurumsal çalışmalar karşısında yasadışı çalışmalar da devam etmektedir.

Zararlı Yazılım (Malware- Spyware)

Malware, Malicious Software kelimelerinin kısaltılmış hali olup zararlı yazılım anlamına gelmektedir. Zararlı yazılım herhangi bir web sitesinden yüklenebileceği gibi kullanıcının bilgisayarına kurulan programlar aracılığı ile de oluşturulmaktadır. Virüs, worm, vb. programlar zararlı yazılımlara örnek teşkil etmektedir. Zararlı yazılımlar sistemsel bütünlüğe zarar verebildiği gibi başka amaçlar için de kullanılabilmektedir. Dijitalleşme, teknoloji kullanıcıları için büyük gelişmeler ve artan karmaşıklık getirmiştir. Ancak aynı zamanda teknolojinin gelişimi, kullanıcıları güvenlik ve mahremiyet ihlalleri konusunda daha yüksek düzeyde riske maruz bırakmıştır.

Messmer, ilk kez 1990 yılında Yisrael Radai tarafından solucan, truva atı ve diğer benzer kötü niyetli varlıkları ifade etmek için kötü amaçlı yazılım terimine öncülük edildiğini belirtmektedir (2023) Kötü amaçlı yazılımlar, yayılma prosedürlerine ve enfekte olmuş sistemde gerçekleştirdikleri faaliyetlere göre karakterize edilmektedir [71]. Siber teknolojilerin ve Yenilenebilir Enerji Kaynaklarının (YEK'ler) yaygın olarak uygulanması, geleneksel güç sistemlerini giderek kötü amaçlı yazılım saldırıları tarafından tehdit edilen yenilenebilir Siber-Fiziksel Güç Sistemlerine (CPPS'ler) dönüştürmüştür (Canavan, 2001; Yohanandhan vd., 2020). Kötü amaçlı yazılım saldırısı,

Siber-Fiziksel Güç Sistemlerine (CPPS'ler) karşı son yıllarda ortaya çıkan yeni bir siber saldırı yöntemidir. CPPS geniş alan izleme ve kontrol için büyük ölçüde siber tesislere dayandığından, bu tür saldırılar genellikle yıkıcı sonuçlara yol açmaktadır (Zhang vd., 2022a). Son zamanlarda mobil telefonlara yüklenerek ortam sesinin dinlenilmesi, görüntü kaydının sağlanması, kiminle ne kadar görüşüldüğü, konuşmanın içeriği, gelen mesajlar ile gönderilen mesajların detayları ilgili yazılımın uygulama özellikleridir. Trojan adı verilen Truva Atı yazılımları bu saldırıda kullanılan yazılımlara örnek olarak gösterilebilmektedir.

Kötü amaçlı yazılımlar kanonik olarak virüsler, solucanlar, Truva atları, rootkitler vb. gibi kategorilerde toplanmıştır. Ancak günümüzün gelişmiş kötü amaçlı yazılımları genellikle farklı işlevlere sahip birçok bileşen içermektedir (Zhang vd., 2022b). Örneğin, aynı kötü amaçlı yazılım bir ana bilgisayar üzerinden yayılırken virüs gibi davranabilir, bir ağ üzerinden yayılırken solucan gibi davranabilir, komuta ve kontrol sunucularıyla iletişim kurarken veya diğer virüslü makinelerle senkronize olurken botnet davranışı sergileyebilir ve kendini gizlerken rootkit davranışı sergileyebilmektedir (Rudd vd., 2017). Malware saldırıları karşısında çeşitli tespit uygulamaları ile güvenlik sistemleri geliştirilmektedir. Bu konuda yapılan çeşitli araştırmalarda makine öğrenmesi üzerinden gerçekleştirilmektedir. Kötü amaçlı yazılım analizi, Makine Öğreniminin önemli ölçüde kullanıldığı en kritik alanlardan biridir. Geleneksel kötü amaçlı yazılım tespit yaklaşımları (Aslan ve Akin, 2022; Siroski ve Honig, 2012; Bin Abbas ve Srikanthan, 2017; Sahoo vd., 2014; Bazrafshan vd., 2013; Zheng vd., 2013) kötü amaçlı yazılım dosyalarının benzersiz tanımlayıcılarının bir veri tabanında tutulduğu ve yeni karşılaşılan şüpheli dosyalardan çıkarılan imzalarla karşılaştırıldığı imzalara dayanmaktadır. Bunun dışında kara kutu öğrenmesi ve Android gibi farklı düzeylerde çözümler üreten olarak çalışmalar da bulunmaktadır. Kara kutu makine öğrenmesi (Barreno vd., 2010; Venugopal ve Hu, 2008) tabanlı tespit modellerini atlayabilen düşmanca kötü amaçlı yazılım örnekleri oluşturmak için MalGAN adlı üretken karşıt ağ (GAN) tabanlı bir algoritma önermektedir. Android tabanlı kötü amaçlı yazılım saldırıları karşı tespit ve çözüm araçları (Hu ve Tan, 2017) güvenlik açıkları, tespit teknikleri ve güvenlik çözümleri konusunda analiz teknikleri, çalışma platformu, veri toplama, operasyonel etki, elde edilen sonuçlar ve ilgili yapay zeka bileşenlerine dayalı yaklaşımları analiz etmektedir.

Fidye-Reklam Engelleme (Ransomeware-Adaware)

Ransomeware Türkçe literatüre fidye yazılımı olarak girmiştir. Temel olarak işlevi hedef gözetmeksizin maksimum sayıda bilgisayara bulaşmasıdır. Bulaştığı bilgisayardaki verileri kripto algoritmalarıyla şifreleyip çalıştırılmak istenildiğinde kullanıcının kripto cüzdan adresine para yatırıldıktan sonra veri şifresinin üzerine kurgulanmış bir sistemdir. Fidye yazılımları ilk olarak 1980'lerin sonunda ortaya çıkmıştır (Li vd., 2020; Qamar vd., 2019) ve 2013'ten bu yana yeniden gündeme gelmiştir. Son zamanlarda, çok sayıda yaygın fidye yazılımı saldırısı, internet üzerindeki çok sayıda kullanıcı sistemi ve işletmede önemli zararlara neden olmuştur (Kharraz, 2016). Fidye yazılımı, önemli dosyaları şifreleyen ve dosyalara erişime izin vermek için kurbandan fidye talep eden veya hedef sistemi tamamen kilitleyerek kullanılamaz hale getiren bir kötü amaçlı yazılım türüdür (Savage vd., Kharraz vd., 2015; Kara ve Aydos, 2022; Gomez-Hernandez vd., 2018; O'Kane vd., 2018; Kirda, 2017). Temel olarak iki tür fidye yazılımı vardır: kripto fidye yazılımı ve kilitli fidye yazılımı (Ferrante vd., 2017; Akbanov vd., 2019). Fidye yazılımı, çalıştırıldığında bir bilgisayarın işlevselliğini devre dışı bırakan veya içindeki dosyaları şifreleyen bir kötü amaçlı yazılım kategorisidir Fidye yazılımı, virüs bulaşmış bilgisayarın masaüstünü kilitlemekten tüm dosyalarını şifrelemeye kadar birçok farklı şekilde çalışır (Li vd., 2020). Adaware, istenmeyen reklam olarak Türkçe' de karşılık bulmuştur. Her internet sayfası ziyaretinde pop-up gösterimi şeklinde reklam görünümü ile çalışmaktadır. Bu durum sıklıkla yaşandığında rahatsız edici bir hal almaktadır. Aynı şekilde enfekte edilen bilgisayarda belirli aralıklarla çıkan reklam gösterimleri de olmadık zamanlarda olmadık içeriklere sahip sayfaların açılmasına neden olabilmektedir. Siber suçlular tarafından fidye yazılımları yaymak için kullanılan en yaygın yöntemlerden bazıları kötü niyetli bağlantılar veya ekler içeren Spam e-posta kampanyaları; İnternet trafiğinin kötü niyetli web sitelerine yönlendirilmesi; Drive-by indirmeleri vb. dir (Baldwin ve Dehghantanha, 2018; Tailor ve Patel, 2017; Monica vd., 2016), Fidye yazılımı tehdidi büyüdükçe, suçluların listesi ve mağdur etme tekniklerinin karmaşıklığı da artmaktadır.

Fidye yazılımı aktörleri (özellikle de RaaS sağlayan aracılar), günde milyonlarca kötü niyetli mesaj gönderebilen güçlü botnet'ler ve savunmasız İnternet Protokolü (IP) adreslerini belirleyen İnternet tarayıcıları da dahil olmak üzere gelişmiş dağıtım tekniklerini giderek daha fazla kullanmaktadır. Ayrıca, Dark Web'de anonimleştirilmiş platformların, sahte e-posta reklamlarının ve ödemeler için kripto para birimlerinin kullanılması, saldırganların dijital ayak izlerini gizlemelerini kolaylaştırmaktadır (Meland, 2020). Suçlular tarafından barındırılan ve amatör saldırganlara bile fidye yazılımı kodlarını indirme ve saldırı başlatma ayrıcalığı veren Hizmet Olarak Fidye Yazılımı (RaaS) sağlayan ağlar vardır. Ayrıca Torlocker, TOX vb. gibi fidye yazılımı kodlarını geliştirmek ve

saldırılar başlatmak için çevrimiçi olarak ücretsiz olarak kullanılabilen geliştirme kitleri de bulunmaktadır (Taylor vd., 2019). Fidye yazılımları sadece teknik bir sorun değil, disiplinler arası bir sorundur (Reshmi, 2021). Suçlular, ilk giriş noktası olarak kurumsal ağlara nüfuz etmek için sosyal mühendislik tekniklerini giderek daha fazla kullanmaktadır. Bu saldırı tipolojisi içerisinde yapılan çalışmalar arasında (Sittig ve Singh, 2016) tarafından kaleme alınan ve bulgularını küçük örneklemli bir anket ve iki mülakata dayandıran bir çalışma bulunmaktadır.

Bunun dışında (Kharraz, 2016) 15 farklı aile içinde kategorize edilmiş bir veri seti kullanarak 2006 ve 2014 yılları arasında vahşi doğada gözlemlenen mevcut fidye yazılımı ailelerinin çoğunu kapsayan bir çalışmada halka açık kötü amaçlı yazılım depolarının manuel ve otomatik olarak taranması ve çeşitli fidye yazılımı örnekleri dahil olmak üzere çoklu kaynaklar kullanılarak oluşturulmuş ve incelemiştir.

Bir başka araştırma (Shinde vd., 2016) kapsamında ise Windows ve Android ortamlarındaki mevcut fidye yazılımı ailelerinden seçilen fidye yazılımı varyantlarının örneklerini analiz ederek, fidye yazılımları tarafından kullanılan şifreleme tekniklerinde önemli bir gelişme olduğunu ve Windows sisteminin Android sistemine oranla ransomware saldırılarının daha yüksek düzeyde tespit edilebilir olduğunu da ortaya çıkarmaktadır.

Zararlı Yazılım (Malicious)

Bu tipoloji[2] davranışsal olarak zarar görme ya da zarar verici davranışları teşvik edici eylem sınıfına girdiği için genel internet erişimlerinde kullanılmaması amacıyla engellenmektedir. Malicious saldırılar, internetteki kötü niyetlilik kimlik hırsızlığı, dolandırıcılık ve ağ veya sistem izinsiz girişlerini (örneğin, bilgisayar korsanlığı, virüsler ve kötü amaçlı yazılımlar) kapsamaktadır (Monica vd., 2016). Genellikle güvenlik ihlallerinin çoğuna neden olduğu düşünülen bu saldırılar iki yoldan biriyle ortaya çıkabilmektedir: Birincisi kullanıcının (saldırganın) bilinen sistemin açıklarından yararlanmak için tamamen meşru işlemler kullanılarak bir saldırı başlatması, ikinci olarak bir kullanıcının doğrudan bilgisayar sistemi kaynakları kategorisine girmeyen bilgi ve kaynakları kullanarak saldırı başlatmasıdır (Xu, 2016). Bu konuda yapılan bazı araştırmalarda Schneider vd., (2011) bir ağın topolojisinde nispeten küçük değişikliklerle ve toplam bağlantı uzunluğunu artırmadan Etkili bir hafifletme yöntemi geliştirerek belirli, kötü niyetli saldırıların tehlikesini önemli ölçüde azaltmanın mümkün olduğunu keşfetmişlerdir (Ray ve Poolsapassit, 2005). Zeng ve Liu, Siber ağların hem düğüm hem de bağlantı arızası ile karışık kötü niyetli saldırılara karşı sağlamlığını doğrulamaya çalışmaktadırlar (2012). Wu vd., (2022) kötü niyetli verilerin doğrudan eyleyicilere bağlanan siber alana enjekte edildiği durumlarda siber-fiziksel sistemler için güvenli kontrol problemini incelemektedir.

Malicious saldırılar, veri sızıntısı ve hırsızlığı, servis kesintileri, verilerin bozulması ve silinmesi, kurumsal itibar kaybı, mali kayıplar, uygulama zafiyetleri ve hatalar, kimlik hırsızlığı ve dolandırıcılık gibi çeşitli sorunlara neden olabilmektedir. Bu saldırılar, kişisel ve kurumsal verilerin ihlali nedeniyle hukuki çatışmalar, sosyo-psikolojik etkilenimler, ulusal güvenlik zafiyetleri gibi ciddi sonuçlar doğurabilen riskli durumlar yaratabilmektedir. Bu saldırıların alt yaş kategorilerine yapılması halinde mahremiyet, siber zorbalık, kötü içeriklere maruz kalma, eğitim süreçlerinin aksaması gibi çeşitli sorunlara neden olabileceği anlaşılmaktadır. Çocuklar ve zararlı eylem gösterebilecek yatkınlığa sahip kişileri engellemek üzere yaygın bir kullanıma sahip yöntemlerden birisidir.

Kripto Hırsızlık (Cryptojacking)

Kullanıcı bilgisayarına bulaştırılan bir yazılım ile cihaz kaynakları kullanılarak madencilik işlemi üzerinden para kazanma yöntemi olarak bahsedilebilmektedir. Etimolojik olarak cryptocurrency ve hijacking olmak üzere iki kelimeden oluşan bu saldırı Cryptojacking olarak adlandırılmaktadır (Kshetri ve Voas, 2022). Cryptojacking, bir saldırganın kar elde etmek için hedef ana bilgisayarda gizlice kripto para madenciliği programını yürüttüğü bir tür kaynak zimmete geçirme saldırısıdır (Xu vd., 2022). Cryptojacking temelde gizli bir ağ tehdidiidir. Bu saldırı güçlü bir saldırgan tarafından hesaplama gücünü artırmak için kullanılabilir ve madenciliğe dayalı herhangi bir blok zinciri için risk oluşturmaktadır (Carlin vd., 2020) Cryptojacking saldırı yöntemleri; "Uç nokta saldırıları, Bir başka yöntem de bir web sitesine ya da birden fazla web sitesine gönderilen bir reklama bir komut dosyası enjekte etmek, Savunmasız sunucuları ve ağ cihazlarını taramak, Yazılım tedarik zinciri saldırıları" (Aponte-Novoa vd., 2022) olarak yer almaktadır. Bir web sitesinde gezinirken bilgisayarın herhangi bir nedenden dolayı aniden çok yavaşladığını fark ederseniz, bilgisayarınız Cryptojacking saldırısına maruz kalmış olabilir. İyi gizlenmesi nedeniyle, her yıl bu tür milyonlarca saldırı olayı meydana gelmektedir (Chickowski, 2022; Musch vd., 2019).

[2] Yetişkin site erişimi olarak adlandırılan davranış, toplum ahlakı ile ilgili bir konuya işaret ettiği için ilgili sitelere erişilmemesi, kişilerin zarar görmesini engelleme yöntemi olarak kullanılmaktadır.

Dashevskyi vd., (2020) mobil cihazların pillerinin hızla tükenebileceğini ve hatta madencilik için yoğun bilgi işlem nedeniyle zarar görebileceğini belirtirken; McCombs vd., (2018) araştırmalarında bazı şirketlerin cryptojacking saldırıları nedeniyle bir süre faaliyet gösteremediğini tespit etmiştir.

Cryptojacking saldırılarını "yeni fenomen" olarak tanımlayan bazı araştırmacılar (McCombs vd., 2018) bu saldırıların büyük oranda kripto para biriminin artan piyasa değeri nedeniyle yükselişte olduğunu belirtmektedir. Web siteleri ile web tarayıcısı şeklinde yapılan bu tür saldırılar önemli güvenlik açıklarına neden olabilmektedir. Web sitelerinde cryptojacking saldırılarında kripto para madenciliği yapmak için Javascript kodu kullanmaktadır. Yasadışı madencilik kodunun kurbanın bilgisayarının tarayıcısında çalışması için kullanıcının virüslü web sitesini tarayıcısına yüklemesi yeterli olarak görülmektedir (Hong vd., 2018).

Tarayıcı içi cryptojacking, web sitesi sahiplerinin bilgisi olmadan popüler web sitelerine kötü amaçlı Javascript kodu enjekte eden ve kendileri için kripto para madenciliği yapan bilgisayar korsanları için bir saldırı yolu olarak hizmet vermektedir. Bu, cryptojacking saldırısı olarak bilinir ve son zamanlarda büyük bir sorun haline gelmiştir (Aponte-Novoa vd., 2022) Tarayıcı tabanlı cryptojacking, fidye yazılımı eğilimlerinin azalmasının ardından hızla büyüyor. Cryptojacking kullanıcının tarayıcısından çalışır ya da popüler web sitelerine yerleştirilebilir, bu da kullanıcının tarayıcısını kullanarak bilgisayarındaki kaynakları kullanmaktadır (Saad vd., 2018; Razali vd., 2019). Saldırganlar tek tek bilgisayarları hedef alarak düşük riskli kötü amaçlı yazılımlar yerleştirmekte ya da bu tür kötü amaçlı yazılımları büyük çevrimiçi portallara yerleştirmek gibi daha basit ve daha popüler bir yolu seçmektedir. Tekiner vd., (2021) tarayıcı uzantıları ve antivirüsler gibi cryptojacking tespit teknikleri, cryptojacking sorununa kısmi bir çözüm sağlayabildiğini zira saldırganların gizleme teknikleri kullanarak veya etki alanlarını veya kötü amaçlı komut dosyalarını nispeten sık sık yenileyerek bunlardan kaçınabilmesini sağladığını belirtmektedirler. Bu yöntem sıklıkla kripto para piyasasının yüksek getiriler sağladığı dönemlerde artmaktadır. Bu saldırıya maruz kalındığında cihaz performansında gözle görülür bir yavaşlama, cihazların aşırı ısınması, kullanılabilir işlem gücünün olmaması nedeniyle kapanan cihazlar, cihazın veya yönlendiricinin üretkenliğinde azalma, elektrik maliyetlerinde beklenmedik artışlar karşılaşılacak sorunlar arasındadır.

Kripto Madencilik (Crypto Mining)

Nakamoto, (2008) kripto para sisteminin geleneksel paranın aksine, bir kripto para biriminin gerçekleştirilmesi, dijital parayı elde etmek için iş kanıtı olarak bilinen belirli bir miktar işin tamamlanmasını gerektiğini, iş kanıtının gerçekleştirilmesi, çok karmaşık ancak uygulanabilir kriptografik algoritmaların hesaplanmasını içerdiği belirtmektedir. Kripto para birimleri üretmek amacıyla iş kanıtını gerçekleştirmek için yapılan bu çalışmaya kripto madenciliği denilmektedir. Madencilik, blok zinciri sistemlerinde, özellikle de Bitcoin gibi kripto para birimlerinde yeni bloklar üretme yöntemidir. Bu sistemde ağ kullanıcıları (madenciler), yeni bir bloğu blok zincirindeki bir önceki bloğa kriptografik olarak bağlamak için hesaplama açısından pahalı bir bulmacayı çözmek zorundadır. Bu bulmacayı çözmenin zorluğu, tüm kullanıcıların birleşik hesaplama gücüne bağlı olduğundan (GPU, FPGA ve ASIC) gibi güçlü makinelere ihtiyaç duyulmaktadır. Madencilere çıkarılan her blok için kripto para verilmektedir. Rüth vd., (2018) bu işlemin, Blok zinciri tabanlı kripto para birimleri, finansal işlemlerin halka açık, kurcalamaya karşı korumalı bir dizi bloğa gömülmesi prensibine dayandığını ve sistemi geliştirmek için, bekleyen işlemleri saklamak üzere sürekli olarak yeni bloklar eklenmesine madencilik denir.

Krishnan vd., (2015) açık ve merkezi olmayan bir sisteme sahip olan ve güvenliği artırmak ve yeni birimlerin oluşturulmasını kontrol etmek için kriptografi kullanan bir dijital para birimi türü olan kripto paranın, geleneksel parasal işlemlerden bir sonraki adımı olarak lanse etmektedir. Madenciler, öngörülebilirliği ve kurcalamaya karşı direnci garanti eden sabit bir blok oranında yeni bloklar üretmek için zorluğu dinamik olarak ayarlanan bir iş kanıtı (PoW) olarak bir kripto bulmacasını çözerler. Srinivasan, siber suçluların mümkün olduğunca az kullanıcı katılımıyla kripto para elde etmenin yollarını bulmakta ve böylece kripto madenciliği saldırılarına başvurmakta olduğunu aktarmaktadır (Srinivasan, 2017).

Cryptomining saldırıları (Mukhopadhyay vd., 2016; Brown, 2016; Carlin vd., 2018; Rüth vd., 2018; Ferrante vd., 2017) için kullanılan tür kötü amaçlı yazılımlar, kurbanların sistemlerini tehlikeye atarak, diğer kötü niyetli faaliyetleri kolaylaştırmak için kullanılabilecek diğer güvenlik açıklarını da açabilmektedir. Bu eylemlerin saldırı boyutunu belirten kripto madenciliği saldırısı (tarayıcı tabanlı), kötü amaçlı yazılımın hedeflenen kurbana değil bir aracıya teslim edilmesi nedeniyle siber saldırılarda bir paradigma değişikliği sunmaktadır. Bu, kurbanda yerleşik bir kötü amaçlı yazılım olmadığından IDS'lerden kaçma gibi önemli bir avantaja sahiptir (Carlin vd., 2018). Tarayıcı tabanlı kripto madenciliği saldırısında üç ana bileşen vardır: saldırgan, kötü amaçlı yazılım ana bilgisayarı

(web sunucusu) ve genellikle bir botnet'in parçası olan kurban'dır. Kripto madenciliği botnet'i, iş kanıtı gereksinimini karşılamak için özel olarak tasarlanmıştır. Çoğu durumda, iş ispatı bireysel bir kurban tarafından gerçekleştirilemez (Zimba vd., 2020). Kripto madenciliği saldırılarında CPU tükenmesi nedeniyle aşırı yüklenme ve aşırı ısınmanın yangınlara bile neden olduğu bildirilmiştir (Becker vd., 2013).

Dolandırıcılık (Scam)

Scam, dolandırıcılık anlamında olup e-postalar genellikle kullanıcıyı maddi zarara uğratmak amaçlı içeriklere sahip metinlerdir. Siber suçun tipik olarak üç ana bileşeni vardır: Siber saldırının hedefi olan mağdur, suçluyu saldırıyı gerçekleştirmeye teşvik eden bir güdü ve suçun gerçekleşmesini sağlayan bir güvenlik açığı veya fırsat (Sun, 2018). Web dolandırıcılığı, "bir web sitesinin yanlış veya kasıtlı olarak yanıltıcı iddialarda bulunduğu bir tür siber güvenlik tehdididir" (Little vd., 2008) Scam suçları, dolandırıcılık konusunda web, kumar, iş ilanı vb gibi alanları kapsamaktadır.

Scam saldırılarını ele alan, çevrimiçi iş ilanları dolandırıcılığı konusunda yapılan bir araştırma, istihdam dolandırıcılığı tespiti konusunu araştırmaktadır. Bu araştırmanın katkısı, IESD adında yeni bir veri kümesi oluşturmak ve bir iş ilanının yasal mı yoksa hileli mi olduğunu belirlemek için davranışsal bağlam tabanlı özellikler önermektir. %90 oranında bir doğrulama elde edilmiştir (Sharifi vd., 2011). Çevrimiçi Aşk Dolandırıcılığı, Whitty ve Buchanan, tarafından "2008 yılında ortaya çıkan nispeten yeni bir dolandırıcılık türü" olarak değerlendirilmektedir (Nindyati ve Nugraha, 2019.) Bu suçta, suçlular çevrimiçi arkadaşlık siteleri aracılığıyla bir ilişki başlatmış gibi davranmakta ve ardından kurbanlarını büyük miktarlarda para dolandırmaktadır Genelde yurt dışında yaşıyor olmak ve bir yakınlarının kaybı sonrası miras kaldığını ancak bu işlemler için birtakım ücretleri ödeyerek ilgili mirasın alınabileceği yönünde gelen e-postalar bu saldırı türünü tanımlamaktadır. Bazı durumlarda herhangi bir loto çekilişini kazanmak veya terör örgütü mensubu kişilerle iletişim kurulması yönünde mesajlar ile de banka bilgilerine ulaşılarak, transfer edilen parasal değerle kayba uğramaya neden olan saldırı şeklidir. Bu saldırı yoluyla herhangi bir şekilde kullanıcı bilgisayarı ya da yazılımsal kaynakları enfekte edilmez ancak kişi zafiyetleri kullanılarak sahip olunan paranın kaybedilmesine yol açmaktadır.

MATERYAL VE YÖNTEM

Ağ toplumu olarak tanımlanan ve internet ile teknolojik araçlar üzerinden şekillenen veri yönetim politikalarının doğal bir sonucu olarak bilgisayar sistemleri üzerinde çeşitli politikalar ortaya çıkmaktadır. Bu politikalar arasında, satış, pazarlama, uygulama, denetim ve uyumluluk politikaları yer almaktadır. Araştırmanın temelini oluşturan siber uzam alanında internet ve web tabanlı sistemlerin ortak noktası olarak IP[3] ve DNS[4] kavramları ön plana çıkmaktadır. DNS Politikaları, eğitim temelli çocuk internet erişim yapısını ve kullanım amaçlarına göre filtreleme yoluyla zararlı içeriklerden koruma prensipleri gerekçesiyle oluşturulabilmektedir. Aynı zamanda kurumsal düzeyde DNS üzerinden zararlı yazılımlara karşı ayrı bir savunma mekanizması geliştirmek ve ticari hakları korumak gibi amaçlarla biçimlendirilmektedir.

Araştırmanın Amacı ve Önemi

Bu araştırma, internet tabanlı gelişen ağ toplumu meselesinde yaşanan olası riskler ve çözüm yollarını ortaya çıkarabilmek için bilgisayar üzerinde gerçekleştirilen bir uygulama tabanlı çözümleme modelini ortaya çıkarmayı hedeflemektedir. Araştırmanın önemi, sistem tabanlı yapılan araştırma projeleri ile kurumsal kaynak kodlu analizlerin yerine tekil kullanıcı bazında nasıl yansıdığını ortaya çıkarabilecek özel bir uygulama modeli ile incelenmesidir. Bu nedenle kurumsal kullanıcılar yerine tekil kullanıcıların olası tehdit ve riskler karşısındaki güncel durumunu ortaya çıkarabilecek örnek- kaynak bir çalışma olacağı düşünülmektedir.

Araştırmanın Evreni ve Örneklemi

Bu araştırma kapsamında ele alınan internet tabanlı hizmetleri kullanan tekil ve çoğul kullanıcılar incelenmektedir. Bu kullanıcılar; kurumsal, kamusal, ticari ve ev tipi kullanıcı olmak üzere dört ana grubu oluşturmaktadır. Söz konusu araştırma evreni içerisinde Statista (2023) tarafından belirlenen 5,4 milyar internet kullanıcısı içerisinde üçte ikisinin internet kullanıcısı olduğu baz alındığında en yaygın kullanım alanına sahip olan ev tipi kullanıcı grupları üzerinden bir analiz geliştirilmeye çalışılmaktadır. Bu bağlamda, araştırma evreni için bu kullanıcı grupları

[3] IP (İng. Internet Protocol), İnternet Protokolü olarak tanımlanan; gerçek hayatta kişilere atanan adı-soyadı ve kimlik numarası tanımlarının internet karşılığı olan, mac adresi ve IP adresi şeklinde tekil kullanıcıya ait bir model olarak karşımıza çıkmaktadır.
[4] DNS (İng. Domain Name System), Alan Adı Sistemi olarak makine dilinde anlaşılabilir formatta rakamlar bütünüyle oluşan IP adresini insanların hatırlayabileceği şekilde anlamlı hale getiren servistir.

seçilmiştir. Tüm kullanıcı gruplarından örneklem olarak ev tipi kullanıcılar belirlenmiştir. Bu kapsamda literatürde de yaygın olarak görülen deneysel nitelikli ve senaryo tabanlı bir saldırı modeli inşa edilerek söz konusu saldırıya ait dönemsel analizleri saptamak üzere örnek bir ev tipi kullanıcının ağ hareketliliğini gösteren teknolojik araçlar belirlenmiştir. Araştırma kapsamında belirlenen çoğul kullanıcının 1 ADSL yönlendirici cihaz, 1 Akıllı TV, 1 Tablet üzerinden DNS sorgu analizi oluşturulmaktadır. Statista (2024) verilerine göre Dünyada ağ penetrasyon değeri açısında Avrupa %97,4 Kuzey Amerika %96,9 oranında gerçekleşirken örnek uygulama alanı olarak seçilen Türkiye'nin %86,5 ile 36. sırada yer alarak önemli bir ağ trafiğine sahip olduğu anlaşılmaktadır.

Araştırmanın Yöntemi ve Veri Toplama Tekniği

Çalışmanın genel içeriği saldırı tipolojileri ile saldırıların düzeylerini niceliksel olarak belirlemek üzere oluşturulduğu için verileri konuşturmak adına içerik düzeyleri üzerinden ölçümleme yapılması daha uygun görülmüştür. Bu bağlamda araştırmada içerik analiz yöntemi seçilmiştir. İçerik analizi; araştırma çalışmalarında elde edilen verilerin nicelik ve niteliksel açıdan analiz edilmesinde sıklıkla tercih edilen bir yöntemdir. İçerik analizi çalışmaları 16. yüzyılda başlayan bir yöntem olmakla birlikte I. ve II. Dünya Savaşı sırası ve sonrasında tüm disiplinlere yönelik kolaylık sağlayan özellikleri itibariyle tercih edilmiştir. İçerik analizi çalışmalarının kavramsal tanımlaması Harold D. Laswell tarafından yapılmış olup alana ait ilk sistemli çalışma, Berelson ve Lazarsfeld tarafından "İletişim Çalışmalarında İçerik Analizi" (1948)'dir. Bu çalışmada ortaya çıkarılan suç tipolojilerinin sınıflandırılması ve analizlerin kategorisel düzeyde incelenmesi konusunda içerik analizi uygulama örnekleri içerik analizinin genel özelliklerini inceleyen (Whitty ve Buchanan, 2012; Berelson ve Lazarsfeld, 1948; Berelson, 1952; Aziz, 1990; Bilgin, 2006; Gökçe, 2006; Krippendorff, 2013) çalışmalar ile çalışmanın analiz modelini belirleyen örnek incelemeler (Yüksel, 2019; Herring, 2004; Abdüsselam vd., 2015; Kolukırık ve Gün, 2020) üzerinden veri setleri değerlendirilmektedir. Yine çalışmada uygulama modülü ve arayüzü geliştirilen yeni bir sistemden suç tipolojileri ve filtreleme listelerine göre engelleme listeleri çerçevelenerek DNS sorguları analiz edilmektedir. Bu kapsamda ayrıca örnek uygulamalar içeren (Yang vd., 2023; Goni, 2022; Lippert, ve Cloutier, 2021; Horan ve Saiedian, 2021) çeşitli çalışmalar da incelenerek suç kavramı ile çözümleme alanlarının genel politikaları da derinlikli olarak analiz edilmektedir.

Araştırmanın Kapsamı ve Sınırlılıkları

Siber uzamda gerçekleştirilen ağ temelli saldırılar, sosyal mühendislik temelli saldırılar ve zararlı yazılım kurulumu (yükleme yapılması) temelli saldırılar üzerinden ortaya çıkan suç tipolojileri bulunmaktadır. Araştırma kapsamında Web ve E-posta tabanlı sanal suç tipolojileri seçilmiştir. Araştırmanın temel sınırlılıklarını Türkiye'de yaşayan kişilere yönelik hizmet veren servisler üzerinde zarar verici eylemlere neden olan verilerin bir aylık araştırması analiz edilmektedir.

Araştırmanın Çözümlemesi

Çalışmanın yapılabilmesi için ilk önce sunucu kurulumunun yapılması gerekmektedir. Bu nedenle 64 bit Rocky Linux dağıtımı temel kurulum ile yapılandırılmıştır. Yapılandırma aşamasında SSH kurulumu ile gerekli uzak terminal erişimi etkinleştirilmiştir. Sunucu ortamı hazırlandıktan sonra DNS kurulumu ve yapılandırılması sağlanmıştır. Bu aşamada kurulum işlemi ile birlikte web ara yüzünden yönetilebilir bir yapı oluşturulmuştur. Daha sonrasında asıl web arayüzü üzerinden çalışmanın temelinde vurgulanan filtreler ve diğer erişim ile ilgili ayarlar gerçekleştirilmiştir. Sonraki adım olarak DNS sorgu istekleri izlenmiştir. Bunların içinde zararlı olan bağlantı istekleri tespit edilerek lokal bir kara liste oluşturulmuştur. Bu sayede oluşturulan tek bir listeden bütün DNS kullanıcıları faydalanarak zararlı bağlantılardan korunmuştur. Ayrıca merkezi olarak kurulabilmesi siber istihbarat açısından da kullanışlı ve etkin olarak son kullanıcı katılımı ile de desteklenebilecektir.

Bu çalışmada geliştirilen sistemde kullanılmakta olan web arayüzüne ait görseller çalışma sırasında kullanılan açık kaynak kodlu yazılımlara aittir. Bununla birlikte web arayüzüne ait yazılım dilinin kodlarında diğer yazılımların entegrasyonu nedeniyle değişiklikler yapılmıştır. Yazılımın çalıştırılması için ihtiyaç duyulan arka planda çalışan python ve bash scripting dilinde yazılmış olan betikler ve kodlar da oluşturulmuştur.

Genel Değerlendirme

DNS yönetimi için öncelikle araştırma deseni oluşturulması adına; genel DNS sorgu tipolojilerinin oluşturulması, sorgulama günlüğü için sorgulama tipolojileri, filtrelenen, işlenen engellenen ve ebeveyn denetimi sağlamak üzere modül oluşturulmaktadır. Araştırma projesinin kod temelli mimari tasarımı noktasında ise DNS için yapılandırma ve şifreleme altyapıları, istemci ayarları, hizmet ayarları ile engel listeleri oluşturulmaktadır. DNS çözümleri için kuruluş aşamasında sorgulama ekranının yönetimi konusunda belli istatistiksel prensipler ve yönergeler

oluşturulmaktadır. Sorgulama konusunda "Tüm Sorgular, Filtrelenen, İşlenen, Engellenen, Engellenen hizmetler, Engellenen tehditler, Ebeveyn denetimi tarafından engellendi ve izin verilen" olmak üzere sınıflandırılma gerçekleştirilmektedir. DNS altyapısının sağlıklı işleyebilmesi için cihaz üzerinde bir ağ yapılandırması ile kurulum sağlanmaktadır.

Filtreleme ile ilgili denetimde alan adlarının engellenmesi, web hizmetinin kullanılmasıyla gezinti koruması için engelleme oluşturulup oluşturulmadığı denetlenmiş, kontrolün ve güvenliğin sağlanması adına SHA256 özet algoritmasını kullanarak DNS kayıtlarının güvenliği ile yönetim kolaylığı için PHP tabanlı bir web arayüzü oluşturulmuştur. Bu arayüz içinde belli sorgulama prensipleri oluşturulmuştur. DNS Sorgulama İlk kurulum Sonrası Prensipleri konusunda tüm sorgu alanlarına ait 9 (dokuz) farklı tipoloji geliştirilmiştir. Bu prensipler; "filtrelenen, işlenen, engellenen, engellenen hizmetler, engellenen tehditler, ebeveyn tarafından engellendi, izin verilen, yeniden yazılan ve güvenli arama" şeklinde sıralanmaktadır.

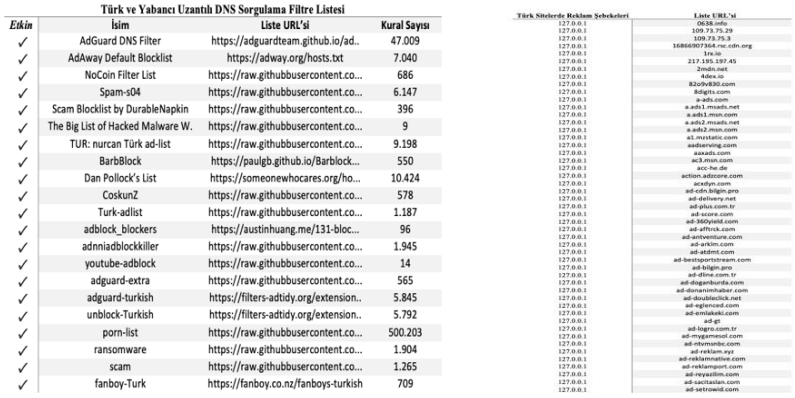
BULGULAR

Araştırma kapsamında oluşturulan arayüz prensiplerinin yanı sıra istatistiksel görünümü sağlamak üzere bir ekran ve sorgulama günlüğü ekranı ayrıca oluşturulmuştur. Aşağıdaki grafiklerde sorgulama ekranı ile sorgulama günlüğü ekranlarının henüz veri olmadan ön izleme hali sunulmaktadır. Bu araştırma, üç aylık bir çalışma sürecinden oluşmaktadır. Araştırmada nitelikli çıktı sağlayabilmek için ilk aşamada 45 günlük süreç içerisinde DNS servisi ile ilgili açık kaynak kodlu tasarım ve yazılımlar incelenmiştir. Açık kaynak kodlu BIND servis yazılımının en güvenli kullanım konfigürasyonu olarak belirtilen DNS-SEC yapılandırması gerçekleştirilmiştir. Bu yapıda DNS kayıtlarını SHA256 özet algoritması ile oluşturulabilecek şekilde konfigürasyon oluşturulmuştur. Ayrıca küresel kullanılan düzeyde kara listelerden Türkiye için uygun olanları tespit edilmiş ve bu listelerin DNS sunucu üzerinde otomatik olarak güncellenmesi sağlanmıştır. Sürecin devamında daha güçlü ve güvenilir bir yapı oluşturmak adına yönetmekte olduğumuz ağa gelen zararlı trafik kaynaklarının IP adresleri ve alan adları yazılan betiklerle sunucu üzerindeki kara listeye eklenmiştir. Bu sayede DNS sunucunun bulunduğu ağa düzenli olarak saldırı gerçekleştiren IP adreslerinin sistem üzerinde sorgu yürütmeleri ve kurum ağına erişimlerinin engellenmesi sağlanmıştır.

Bu engelleme işlemi oluşturulan güvenli DNS sunucusunun günümüzde kullanılan güvenlik duvarlarının birçoğunda bulunan dinamik engelleme özelliği sayesinde iç ağdan zararlı faaliyet gösteren IP adreslerine ve alan adlarına yapacakları trafik engellemiş olup dış ağ üzerinden kayıtlı IP adresi ve alan adlarından kuruma doğru erişim istekleri güvenlik duvarı sayesinde engellenmiştir. Sistemin analiz süreci boyunca 15 günlük ilk veri akışı için izleme süreci oluşturulmuş ve sistem kaynak tüketimine neden olan betiklerdeki ya da kodlardaki hatalar ile ilgili kısımların düzenlenmesi ve kuralların yeniden yazımı gerçekleştirilmiştir. Söz konusu kurallar, false pozitif olarak adlandırılan ve hatalı çıktıya neden olan hatta zararlı olduğu düşünülmesine rağmen sistem tarafından kullanılan DNS filtreleme kuralları ile güvenlik duvarında kullanılan listelerin içerisinde geçen IP adreslerini düzenlenmesini ifade etmektedir. Örnek olarak zararlı yazılım davranışı sergileyen bir isteğe ait IP adresi küresel olarak konumlandırılmış bulut hizmeti veren sunucuların IP adresini engellemek aynı IP adresine sahip herhangi bir zararlı davranış sergilemeyen alan adının da engellenmesine neden olabilmektedir. Bu sebeple bir IP adresine atanmış birden fazla ve farklı hizmetleri yürütebilmek amacıyla kullanılan alan adlarının erişim engeli sorunu yaşamasının önüne geçilmesi sağlanmıştır.

Çalışmada DNS filtrelemesi olarak adlandırılan alan adları, 5651 sayılı kanun kapsamında konusu suç teşkil eden (Yetişkin içerik, yasadışı kumar ve bahis siteleri gibi) alan adları ile USOM (Ulusal Siber Olaylara Müdahale) tarafından yayınlanan alan adı ve IP listesi olarak belirtilmektedir. Kanunlar çerçevesinde zararlı faaliyet gösteren sistem ve sunuculara erişimin engellenmesi ilk olarak DNS servisi düzeyinde gerçekleştirilmektedir.

Bu kapsamda "DNS Sorgu Filtre İsimleri Listesi Görünümü" ile DNS Sorgu Türk ve Yabancı İstenmeyen Reklam Engelleme Listeleri oluşturulmuştur. Aşağıda yer alan grafiklerde bu listelere yer verilmektedir. Araştırmanın ikinci aylık sürecinde ise ilk test süreçleri ile kısıtlı sorgulama yapılarak veri akışı ve verilerin kurallar dizgesi ile nitelik kazanma parametreleri denetlenmiştir.



Türk ve Yabancı Uzantılı DNS Sorgulama Filtre Listesi

Etkin	İsim	Liste URL'si	Kural Sayısı
✓	AdGuard DNS Filter	https://adguardteam.github.io/ad..	47.009
✓	AdAway Default Blocklist	https://adway.org/hosts.txt	7.040
✓	NoCoin Filter List	https://raw.githubbusercontent.co...	686
✓	Spam-s04	https://raw.githubbusercontent.co...	6.147
✓	Scam Blocklist by DurableNapkin	https://raw.githubbusercontent.co...	396
✓	The Big List of Hacked Malware W.	https://raw.githubbusercontent.co...	9
✓	TUR: nurcan Türk ad-list	https://raw.githubbusercontent.co...	9.198
✓	BarbBlock	https://paulgb.github.io/Barblock...	550
✓	Dan Pollock's List	https://someonewhocares.org/ho...	10.424
✓	CoskunZ	https://raw.githubbusercontent.co...	578
✓	Turk-adlist	https://raw.githubbusercontent.co...	1.187
✓	adblock_blockers	https://austinhuang.me/131-bloc...	96
✓	adnniadblockkiller	https://raw.githubbusercontent.co...	1.945
✓	youtube-adblock	https://raw.githubbusercontent.co...	14
✓	adguard-extra	https://raw.githubbusercontent.co...	565
✓	adguard-turkish	https://filters-adtidy.org/extension..	5.845
✓	unblock-Turkish	https://filters-adtidy.org/extension..	5.792
✓	porn-list	https://raw.githubbusercontent.co...	500.203
✓	ransomware	https://raw.githubbusercontent.co...	1.904
✓	scam	https://raw.githubbusercontent.co...	1.265
✓	fanboy-Turk	https://fanboy.co.nz/fanboys-turkish	709

Türk Sitelerde Reklam Şebekeleri — Liste URL'si

127.0.0.1	0638.info
127.0.0.1	109.73.75.29
127.0.0.1	109.73.75.3
127.0.0.1	1686907364.rsc.cdn.org
127.0.0.1	1rx.io
127.0.0.1	217.195.197.45
127.0.0.1	2mdn.net
127.0.0.1	4dex.io
127.0.0.1	82o9v830.com
127.0.0.1	8digits.com
127.0.0.1	a-ads.com
127.0.0.1	a.ads1.msads.net
127.0.0.1	a.ads1.msn.com
127.0.0.1	a.ads2.msads.net
127.0.0.1	a.ads2.msn.com
127.0.0.1	a1.mzstatic.com
127.0.0.1	aadserving.com
127.0.0.1	aaxads.com
127.0.0.1	ac3.msn.com
127.0.0.1	acc-he.de
127.0.0.1	action.adcrore.com
127.0.0.1	acxdyn.com
127.0.0.1	ad-cdn.bilgin.pro
127.0.0.1	ad-delivery.net
127.0.0.1	ad-plus.com.tr
127.0.0.1	ad-score.com
127.0.0.1	ad-360yield.com
127.0.0.1	ad-affinity.com
127.0.0.1	ad-antventure.com
127.0.0.1	ad-arkim.com
127.0.0.1	ad-atdmt.com
127.0.0.1	ad-bestsportstream.com
127.0.0.1	ad-bilgin.pro
127.0.0.1	ad-dline.com.tr
127.0.0.1	ad-doganburda.com
127.0.0.1	ad-donanimhaber.com
127.0.0.1	ad-doubleclick.net
127.0.0.1	ad-eglenced.com
127.0.0.1	ad-emlakeki.com
127.0.0.1	ad-gt
127.0.0.1	ad-logro.com.tr
127.0.0.1	ad-mygamesol.com
127.0.0.1	ad-otvmonbc.com
127.0.0.1	ad-reklam.xyz
127.0.0.1	ad-reklamnative.com
127.0.0.1	ad-reklamport.com
127.0.0.1	ad-reyazilim.com
127.0.0.1	ad-sacitaslan.com
127.0.0.1	ad-setrowid.com

(a) (b)

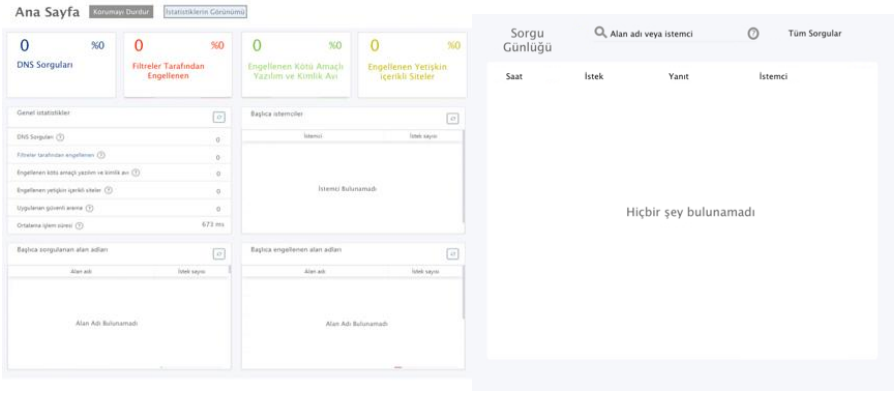
Şekil 1(a). DNS Sorgulama Filtre İsimleri Listesi Görünümü, **(b)** DNS Türk Sorgu Ve İstenmeyen Reklam Engelleme Listesi Görünümü

Araştırmanın üçüncü aylık dönemi olan 1-30 Haziran 2023 tarihlerinde ise tam ölçümlü ve kesinlikli veri akışları dizgesi ile sorgu ve diğer analizlerin takibi yapılmıştır. Sorgulama konusunda; dört temel değer sistemi oluşturularak DNS Sorgu Sayısı, Engel Sayısı, Kötü Amaçlı Yazılım ve Kimlik Avı ile Yetişkin İçerikli Siteler şeklinde sistem oluşturulmuştur

TÜRK VE YABANCI LİSTE URL'Sİ

mikocin. site	kill3rr.com
ip80-ip-51-195-81.eu	meniskon.com
exmo.co.in	findatingall.site
chat.warlab.info	conhost.pw
a2ecommerce.com	brokenbones.ga
346211-cw53847. tmweb.ru	searchtool.space
343637-cg89835. tmweb.ru	f0457098.xsph.ru
340039-co76336. tmweb.ru	f0457102.xsph.ru
trilfy.ru	45-76-47-204.plesk. page
cloacakoshiki.myjino.ru	slweb.xyz
qlaston.net	pma.finansist.xyz
mjlog-vn.com	pma.fin.ex2life.cf
mecharnise.ir	panelaragon.es
kibossuqar.ir	outlook.al
goldrealestate.ga	mc.desmine.ru
a0458390.xsph.ru	ip140.ip-178-32-145.eu
truegreen-cn.com	ip101.ip-51-75-58.eu
malletmissile.ru	finansist.xyz
ldokja.xyz	fin.ex2life.cf
greenzing.top	ex2life.cf
funtionalrejh.com	downersnow.tk
cubbiesdo.ru	321042-cy13670.tmweb.ru
www.eos-numerique.com	183.123.235.35.bc.googleusercontent.com
voceconfia.com.tr	vm1265017.ssd.had.yt
mailerphppro.blogspot.com	s176448.hostiman.com
elhusseinyusmleprep.com	lcba5a9.justinstallledpanel.com
pcmall.ca	brokenbones.ml
brokenskull.gq	brokenbones.cf
brokenskull.cf	lfa3231e. justinstalledpanel.com
krockabread.com	Ec2-34-223-60-188.us-west-2.compute.amazonaws.com
phiheatings.ir	

Şekil 2. DNS Sorgu Yabancı İstenmeyen Reklam Engelleme Listesi Görünümü



(a) (b)

Şekil 3(a). DNS Sorgulama Ekranının İlk Kurulum Sonrası İstatistiksel Görünümü**, (b)** DNS Sorgulama Günlüğünün İlk Kurulum Sonrası İstatistiksel Görünümü

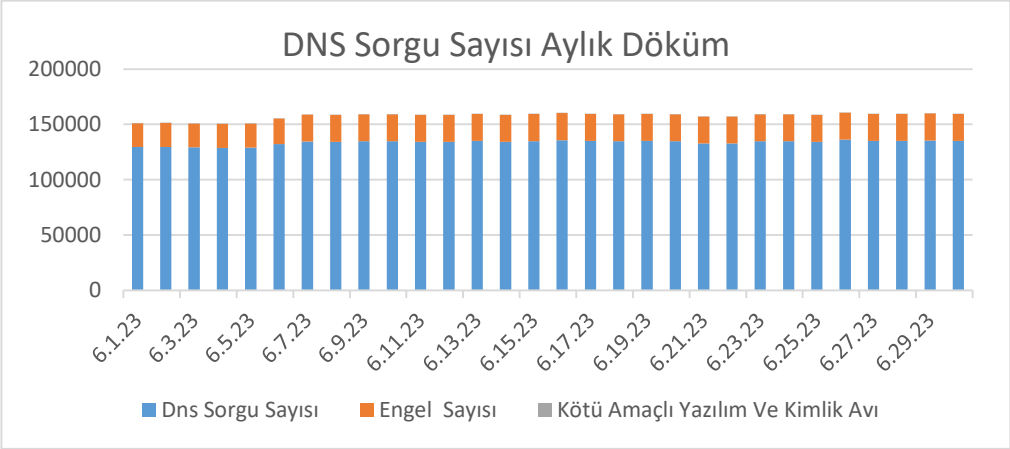
Araştırma kapsamında hazırlanan uygulamanın kurulumu sonrasında Yukarıda **Şekil 3(a)** olarak yer alan şekilde; "DNS Sorgu Sayısı, Engel Sayısı, Kötü Amaçlı Yazılım ve Kimlik Avı ile Yetişkin İçerikli Siteler" şeklinde üst sekmede bir bölüm alt sekmelerde ise "Genel istatistikler, başlıca istemciler, Başlıca sorgu alan adları ile başlıca engellenen alan adları" temelinde bir sistem oluşturulmuştur. Aşağıda yer alan **Şekil 3(b)** üzerinde yer alan "Sorgu Günlüğü" bölümünde ise ilk ekran görünümü olarak herhangi bir verinin bulunmadığı başlangıç grafiğinde "Hiçbir şey bulunamadı" ibaresi yer almaktadır.

Aşağıda yer alan **Tablo 1'**de "DNS Sorgularının Bir Aylık Toplam ve Ortalama Değer Görünümü" incelendiğinde ilk beş günlük dilimde en düşük sorgu sayısının olduğu, sorgu sayısında ayın ortasına karşılık gelen 16.06.2023 ve 17.06.2023 tarihlerinde en yüksek sorgulama sayısına ulaşıldığı görülmektedir. DNS sorgu sayılarında toplamda 4.010.360 rakamına ve 133.678 ortalama değere karşılık gelen istatiksel veriler elde edilmiştir. Engel sayılarında da benzer bir şekilde aynı zaman parametrelerinde ayni değer özelliğine rastlanıldığı, 15.06.2023 ile 16.06.2023 tarihlerinde en yüksek ve aynı sayıda engel düzeye ulaşıldığı anlaşılmaktadır. Engel sayılarında toplamda 715.989 rakamına ve 23,866 ortalama değere karşılık gelen istatiksel veriler elde edilmiştir. Kötü amaçlı yazılım ve kimlik avı değerlerinde ilk gün içinde 161 rakamına en yüksek değer olarak ulaşıldığı, ikinci olarak 17.06.2023 tarihinde 152 ile ikinci en yüksek değere ulaşıldığı, toplam sayının 2944 olduğu, genel ortalamanın ise 98 olarak ortaya çıktığı görülmektedir. Yetişkin içerikli sitelerde ise yapılan etkin filtrelemelere bağlı olarak herhangi bir veri akışının olmadığı dolayısıyla veri sağlanmadığı anlaşılmaktadır.

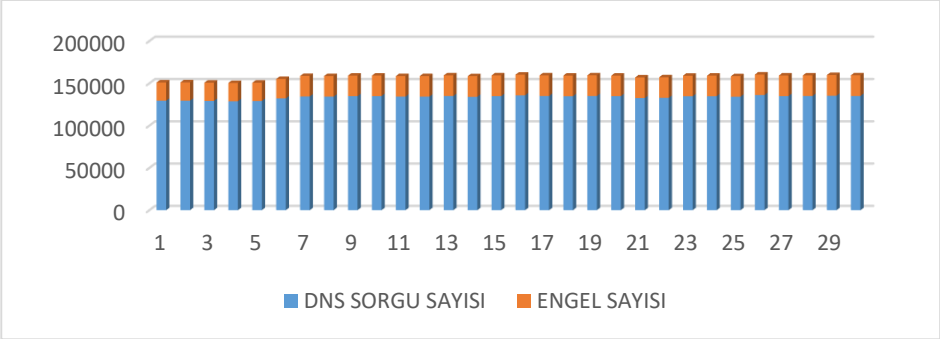
Tablo 1. DNS Sorgularının Bir Aylık Toplam Ve Ortalama Değer Görünümü

DNS Sorgularının Bir Aylık Toplam ve Ortalama Değer Görünümü				
DNS Sorgu Tarihi	**DNS Sorgu Sayısı**	**Engel Sayısı**	**Kötü Amaçlı Yazılım Ve Kimlik Avı**	**Yetişkin İçerikli Siteler**
01.06.2023	129436	21612	161	0
02.06.2023	129515	21640	94	0
03.06.2023	129209	21600	86	0
04.06.2023	128808	21614	74	0
05.06.2023	129131	21621	72	0
06.06.2023	132189	23008	85	0
07.06.2023	134442	24330	110	0
08.06.2023	134290	24328	107	0
09.06.2023	134848	24320	132	0
10.06.2023	134866	24341	85	0
11.06.2023	134259	24321	81	0
12.06.2023	134244	24330	79	0
13.06.2023	134985	24419	116	0
14.06.2023	134084	24420	96	0
15.06.2023	134861	24516	95	0
16.06.2023	135763	24516	96	0
17.06.2023	135024	24389	152	0
18.06.2023	134792	24392	90	0
19.06.2023	135034	24464	83	0
20.06.2023	134813	24363	78	0
21.06.2023	132673	24318	77	0
22.06.2023	132856	24294	112	0
23.06.2023	134729	24297	100	0
24.06.2023	134790	24322	86	0
25.06.2023	134197	24298	96	0
26.06.2023	136166	24298	81	0
27.06.2023	134932	24363	92	0
28.06.2023	134970	24383	119	0
29.06.2023	135366	24451	117	0
30.06.2023	135088	24421	92	0
TOPLAM SAYI	4010360	715989	2944	0
ORTALAMA DEĞER	133678,6667	23866,3	98,13333333	0

Aşağıda yer alan "DNS Sorgu Bir Aylık Sorgu, Engel ve Kötü Amaçlı Yazılım ve Kimlik Avı Pasta Görünümü" grafiğinde DNS sorgu sayısı ile engel, kötü amaçlı yazılım ve kimlik avı değerlerinde belirgin düzeyde farklılıklar olduğu ortaya çıkmaktadır. Yine "DNS Sorgu Bir Aylık Sorgu ve Engel Pasta Görünümü" grafiğinde sadece iki değer olarak sorgu ve engel sayılarının ikili analizinde yüksek ve farklı düzeylerde değerlere erişildiği görülmektedir.

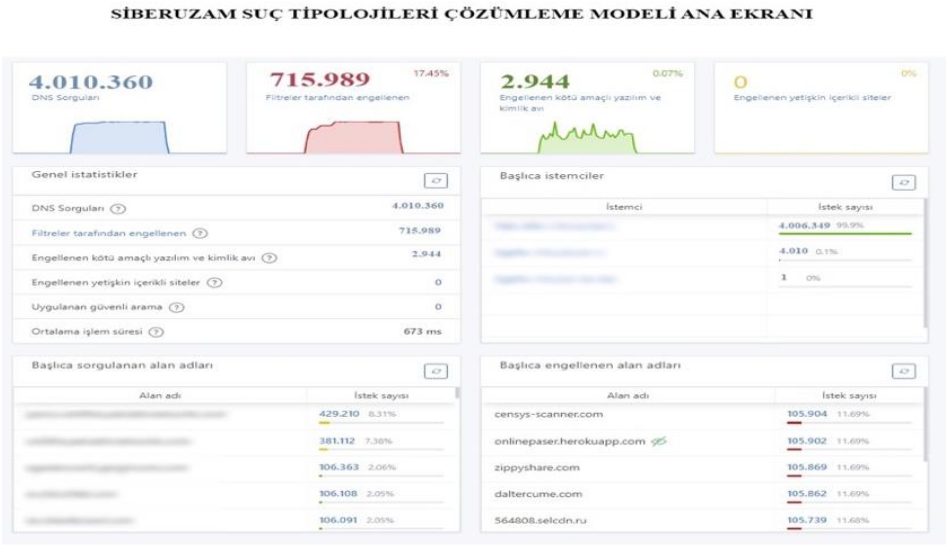


Şekil 4. DNS Sorgularının Bir Aylık Sorgu, Engel Ve K.A.Y.K.A Pasta Görünümü



Şekil 5. DNS Sorgularının Bir Aylık Sorgu Ve Engel Pasta Görünümü

Araştırma kapsamında "Sorgu, Engel ve Kötü Amaçlı Yazılım ve Kimlik Avı (K.AY.K. A) Bir Aylık Çizgisel Analiz Görünümü" ayrı ayrı değerlendirildiğinde; DNS Sorgu sayısında bir aylık incelemelerde yükseliş yönünde bir çizgisel değere sahip olduğu anlaşılmaktadır. DNS Sorgu, Bir Aylık Engel Sayılarına ait grafik incelendiğinde ilk haftadan itibaren yükselişe geçen daha sonra yatay eksende seyreden çizgisel değere sahip noktasal yükseliş ortaya çıkmaktadır.



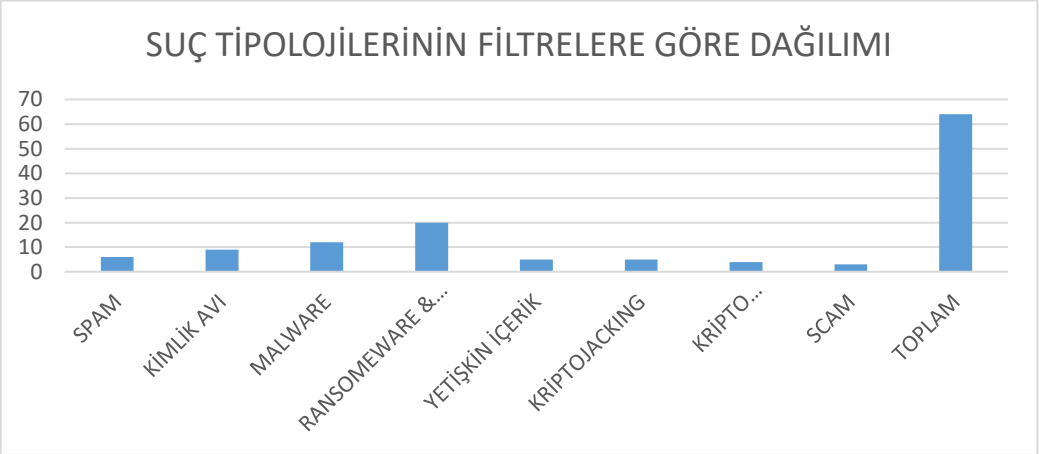
Şekil 6. DNS Sorgu Bir Aylık İzleme Sonrası Genel İstatistik Görünümü

Bilimsel çalışmaların en önemli uygulama alanlarından birisi olarak bu çalışma özelinde yeni bir yazılım şeklinde oluşturulan sistem arayüzü üzerinden tüm veriler ışığında elde edilen **"**DNS Sorgu Bir Aylık İzleme Sonrası Genel İstatistik Görünümü" değerlendirildiğinde; sadece bir aylık analiz sürecinde yüksek ortalama değere sahip olduğu anlaşılmaktadır. Zira, "sorgulama, engelleme, kötü amaçlı yazılım ve kimlik avı" ölçütlerinde suç tipolojilerinin filtreleme sistemi üzerinden hangi alanlarda suç tipolojileri ile zararlı bir yapıya dönüşebileceği renklendirilmiş bir ana ekran ile ortaya çıkmaktadır.

Tablo 2. Suç Tipolojileri Filtre Dağılım Sayılarının Genel Görünümü

Filtreleme Oranlarının Görünümü			
No	**Türü**	**Oranı**	**Yüzdesi**
1	Spam	6	9,37
2	Kimlik Avı	9	14,06
3	Malware	12	18,75
4	Ransomeware ve Adaware	20	31,25
5	Malicious Zararlı Yazılım Yetişkin İçerik	5	7,81
6	Kriptojacking	5	7,81
7	Kripto Madenciliği	4	6,25
8	Scam	3	4,68
Toplam	8	**64**	**%100**

Yukarıda yer alan "Suç Tipolojileri Filtre Dağılım Sayılarının Genel Görünümü ve Grafiksel Genel Görünümü" verileri değerlendirildiğinde; 8 tane tür olduğu görülmektedir. Bu türler; Spam, Kimlik Avı, Malware, Ransomeware ve Adaware, Yetişkin içerik, Kriptojacking, Kripto Madenciliği ve Scam olmak üzere belirlenmiş ve oran ve yüzde değerleri açısından farklı sayısal ölçümlere ulaşılmıştır. Spam oranları 6 ve yüzdesi %9,37; Kimlik Avı oranları 9 ve yüzdesi 14,06; Malware oranları 12 ve yüzdesi 18,75; Ransomeware ve Adaware oranları 20 ve yüzdesi 31,25; Yetişkin içerik oranları 5 ve yüzdesi 7,81; Kriptojacking, oranları 5 ve yüzdesi 7,81; Kripto Madenciliği oranları 4 yüzdesi 6,25 ve Scam oranları 3 yüzdesi ise 4,68 şeklinde sıralanmaktadır.



Şekil 7. Suç Tipolojileri Filtre Dağılım Sayılarının Grafiksel Genel Görünümü

Yukarıda yer alan "Suç Tipolojileri Filtre Dağılım Sayılarının Genel Görünümü ve Grafiksel Genel Görünümü" verileri değerlendirildiğinde; 64 toplam filtreleme listesi içinde yapılan analize göre 48 adet yabancı filtre (%87,3) ve Türk filtre olarak 7 adet (%12,7), 9 adet ortak filtre tipolojisi özelliği gösteren filtreler olmak üzere belirtilen oranlarda gerçekleştiği ortaya çıkmaktadır.

SONUÇLAR

Yeni nesil ağ teknolojilerinde internet tabanlı gelişim ile birlikte kullanıcıların eğilimleri evrilmektedir. Günümüzde dijitalleşme çabaları sanal düzlemde karşılık bulmaktadır. Farklı kullanıcı tipolojilerinin oluşması sonucu, içerik ve siber uzamda mahremiyet konusunda beklentiler değişebilmektedir. Söz konusu beklentiler, siber dünyada sanal kullanıcıların suç ve zarar konularıyla yüzleşmeleri nedeniyle güvenli internet kullanma tercihlerinde de belirleyici rol üstlenebilmektedir.

Bu çalışma, internet kullanıcılarının kendi internet ağları üzerinden gerçekleşen dijital hareketlerinin IP ve DNS örnekleri üzerinden suç tipolojileri karşısında yaşayabileceği siber saldırı ve zorbalık nedeniyle hangi muhtemel suç tipolojileriyle karşılaşabileceklerini ve muhtemel çözüm önerilerini ortaya çıkarabilmek üzere DNS yapıları üzerinden kural ve filtreleme yoluyla oluşturulan ağ hareketine odaklanmaktadır.

Araştırma kapsamında ilk aşamada DNS ve IP arasındaki teknik ilişkiyi ortaya çıkarabilmek üzere yapılan test süreçlerinde tek tip dijitalleşme ve kullanıcı profili olmadığı ortaya çıkmaktadır. Yapılan arayüz tasarımında ve uygulama çalışmasında elde edilen bir aylık verilere göre özellikle içerik endüstrisinin reklam ve dolandırıcılık yoluyla hedef kitleyi temsil eden kullanıcılar üzerinde kurduğu baskılayıcı yapının suç tipolojilerinin niceliksel oranlarıyla örtüştüğü anlaşılmaktadır. Zira, araştırma kapsamında bir aylık veriler içerisinde Tablo 2'de yer aldığı üzere reklam ve dolandırıcılık tabanlı suç tipolojisinin 20 oran ve %31,25 ile en yüksek değere sahip olması, içerik tabanlı erişimler üzerinden kitlelere karşı yapılan saldırıların daha yüksek risk barındırdığını da ortaya çıkarmaktadır. Siber uzamda gerçekleşen tüm saldırılar ile suç kavramının dijital alanı ve sanal kimlikleri de etkilemesiyle muhtemel teknik ve hukuki çözümlerin üretilmesinin de zorunlu hale geldiği görülmektedir. Yine çalışma kapsamında, DNS üzerinden ağ temelli suçlara ilişkin yapının genel görüntüsünün ortaya çıkarılması, mahremiyet ve kullanıcı tabanlı koruma yöntemlerinin iyileştirilmesinin nasıl sağlanabileceği ile ilgili kurallar, satırlar ve filtreleme biçimleriyle anlamlı ilişkilendirilmektedir.
Kullanıcı tabanlı DNS filtresinin onarılması ve DNS sunucusu üzerinden yürütülecek tüm sorguların gizliliği için SSL (İng. Secure Socket Layer) adı verilen Güvenli Giriş Katmanı gibi güvenli web sorgulama yapılarının oluşturulması gerekmektedir. Bu çözümleme yöntemleri, internete erişim için kullanılan yönlendirici ya da güvenlik duvarı üzerinde gerekli önlemler alındıktan sonra ilgili yapının daha güvenilir olmasını ve ağda daha iyi hizmet verebilir hale getirilebilmesini sağlayabilmektedir.

Sonuç olarak, analiz çerçevesinde ev tipi çoğul kullanıcı örneği üzerinden DNS yapısındaki "sorgu, engelleme, zararlı içerik ve kimlik avı" yapılarındaki değişim yüzdeleri siber suç tipolojilerinin genel yönelim yapılarını da ortaya çıkarmaktadır. İnternet tabanlı teknolojilerinin tam anlamıyla güvenli olmadığı, güvenli internet alanının sadece hizmet satın alma ve yazılımsal bir süreç içermediği aynı zamanda kullanıcının bilinç düzeyi, araştırmacı yapısı ve ağ sistemleri üzerinde engelleyici güvenli çözümlerinin üretilmesindeki çabalarına göre değişiklik gösterdiği de görülmektedir.

KAYNAKLAR

Abdüsselam, M. S., Burnaz, E., Ayyıldız, H., & Demir, İsmail K. (2015). web teknolojilerinin e-ticaret ortamlarında kullanımı ile ilgili içerik analizi: Türkiye'deki ilk 500 e-ticaret sitesi. *KTÜ, SBE Sos. Bil. Dergisi, 2015(10),* 263-284.

Abide, Ö. F., & Gelişli, Y. (2020). Sosyal bilgiler ders kitaplarının ve öğretim programlarının çocukların güvenli internet kullanımları açısından incelenmesi. *JRES*, 7(1), 248-269.

Akbanov, M., Vassilakis, V.G., & Logothetis, M.D. (2019). Ransomware detection and mitigation using software-defined networking: The case of WannaCry. *Computers & Electrical Engineering,* 76, 111-121. https://doi.org/10.1016/j.compeleceng.2019.03.012

Akbulut, Y., Dursun, Ö.Ö., Dönmez, O., & Şahin, Y.L. (2016). In search of a measure to investigate cyberloafing in educational settings. *Computers in Human Behavior,* 55, 616-625.

Akgün, E. (2022). Güvenli internet ile ilgili tezlerdeki yöntemsel eğilimlerin sistematik incelenmesi. *Instructional Technology and Lifelong Learning, 3(1),* 64-87. https://doi.org/10.52911/itall.1062981

Akman, T. (1982). *bilimler bilimi sibernetik.* Karacan Yayıncılık.

Akyüz, A., & Koç, Z. (2020). Empati yönelimli siber zorbalık psiko-eğitim programının lise 9. ve 10. sınıf öğrencilerinin siber zorbalık ve empati düzeylerine etkisi. *Gazi Üniversitesi Gazi Eğitim Fakültesi Dergisi, 40(1),* 75-111. https://doi.org/10.17152/gefad.695923

Alan, H. (2019). Sosyal ağ kullanımı yoğunluğu ve sanal kaytarma davranışları: Üniversite öğrencileri üzerine bir inceleme. Çağdaş Yönetim Bilimleri Dergisi, 6(2), 112-129. https://dergipark.org.tr/tr/pub/cybd/issue/49666/495333

Allen, M. (2006). *Social engineering: A Means to violate a computer system.* Tech. Rep., SANS Institute.

Anandarajan, M., & Simmers, C. A. (2005). Developing human capital through personal web use in the workplace: Mapping employee perceptions. *Communications of The Association For Information Systems,* 15, 776-791. https://doi.org/10.17705/1CAIS.01541

Androutsopoulos, I., Paliouras, G., Karkaletsis, V., Sakkis, G., Spyropoulos, C.D., & Stamatopoulos, P. (2000). Learning to filter spam e-mail: a comparison of a naive bayesian and a memory-based approach. Zaragoza H, Gallinari P, Rajman M. (Eds.), *Proceedings of the workshop, Machine Learning and Textual Information Access,* (pp.1-13), 4th European Conference on Principles and Practice of Knowledge Discovery in Databases (PKDD-2000), Lyon, France, September 2000.

Aponte-Novoa, F.A., & Villanueva-Polanco, R. (2022a). On proof-of-accuracy consensus protocols. *Mathematics, 2022(10),* 2540, 1-27. https://doi.org/10.3390/math10142504

Aponte-Novoa, F.A, Povedano Álvarez, D., Villanueva-Polanco, R., Sandoval Orozco, A.L., & García Villalba, L.J. (2022b). On detecting cryptojacking on websites: Revisiting the use of classifiers. *Sensors, 22(23),* 9219, 1-15. https://doi.org/10.3390/s22239219

APWG. (Anti-Phishing Working Group). (2013). Phishing Activity Trends Report-4th Quarter 2013. http://apwg.org/resources/apwg-reports Accessed:17.11.2023.

Arabacı, İ. (2017). Investigation faculty of education students cyberloafing behaviors in terms of various variables. *The Turkish Online Journal of Educational Technology, 16(1),* 72-82.

Arachchilage, N.A.G, & Love, S.A (2013). Game design framework for avoiding phishing attacks. *Computers in Human Behavior 29(2013)* 706-714. http://dx.doi.org/10.1016/j.chb.2012.12.018

Arıcak, T., Siyahhan, S., Uzunhasanoglu, A., Saribeyoglu, S., Çıplak, S., Yılmaz, N., & Memmedov, C. (2008). Cyberbullying among Turkish adolescents. *CyberPsychology Behavior, 11(3),* 253-261. https://doi.org/10.1089/CPB.2007.0016

Aslan, A. & Karakuş Yılmaz, T. (2017). Türkiye'de güvenli internet kullanımına yönelik gerçekleştirilen uygulamalar. *Dumlupınar Üniversitesi Sosyal Bilimler Dergisi, 53. Sayı-Temmuz 2017*, 121-143.

Aslan, O, & Akin, E. (2022). Malware detection method based on file and registry operations using machine learning. *Sakarya University Journal of Computer and Information Sciences, 5(2),* 134-146. https://doi.org/10.35377/saucis...1049798

Aziz, A. (1990). *Araştırma yöntemleri-teknikleri ve iletişim.* A. Ü Siyasal Bilgiler Fakültesi ve Basın-Yayın Yüksekokulu Basımevi.

Bağrıyanık, M. F. (2018). Dijital alanın tipolojileri: dijital kültüre dair sosyolojik bir okuma, Yüksek Lisans Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya, 111s.

Baldwin, J., & Dehghantanha A. (2018). Leveraging support vector machine for opcode density based detection of crypto-ransomware. In *Cyber Threat Intelligence*, Cham: Springer, 107-136, https://doi.org/10.1007/978-3-319-73951-9_6

Bargh, J.A., & McKenna, K.Y.A (2004). The internet and social life. *Annual Review of Psychology, 55,* 573-590.

Barreno, M., Nelson, B., Joseph, A., & Tygar, J. (2010). The security of machine learning. *Machine Learning, 81,* 121-148.

Baykara, M., & Gürel, Z.Z. (2018). Detection of phishing attacks. 2018 *6th International Symposium on Digital Forensic and Security* Antalya, Turkey, 2018, (pp.1-5), ISDFS. https://doi.org/10.1109/ISDFS.2018.8355389

Bazrafshan, Z., Hashemi, H., Fard, S.M.H., & Hamzeh, A. (2013). A Survey on heuristic malware detection techniques. In *IEEE Conference on Information and Knowledge Technology,* (pp.113-120), IEEE.

Becker, J., Breuker, D., Heide, T., Holler, J., Rauer, H.P., & Böhme, R. (2013). Can we afford integrity by proof-of-work? Scenarios inspired by the Bitcoin currency. *The Economics of Information Security and Privacy*; 2013, Springer: Berlin, Heidelberg, 135-156.

Becker, T.E., & Martin, S.L. (1995). Trying to look bad at work: Methods and motives for managing poor impressions in organisations, *Academy of Management Journal, 28(1),* 174-200.

Berelson, B. (1952). *Content analysis in communication research*. Free Press.

Berelson, B., & Lazarsfeld, P. F. (1948). *The Analysis of communication content.* University of Chicago and Columbia University.

Bergholz, A., DeBeer, J., Glahn, S., Moens, MF, Paaß, G., & Strobel, S. (2010). New filtering approaches for Phishing e-mail. *Journal of Computer Security, 18(1),* 7-35.

Beugre, C. D., & Daeryong, K. (2006). Cyberloafing: Vice or Virtue? Mehdi Khosrow Pour (Ed.), *Emerging Trends and Challenges in Information Technology Management,* (pp.834-835), Idea Group Inc.

Bhavsar, V., Kadlak, A., & Sharma, S. (2018). Study on phishing attacks. *International Journal of Computer Applications, (0975-8887), 182(33),* December 2018, 27-29.

Bhowmick, A., & Hazarika, S. (2018). E-Mail spam filtering: a review of techniques and trends, Bhowmick, Kalam A, Das S, Sharma K. (Eds.) *Advances in Electronics, Communication and Computing. Lecture Notes in Electrical Engineering,* Vol 443, (pp.583-590), Springer, Singapore. https://doi.org/110.1007/978-981-10-4765-7_61

Bilgin, N. (2006). *Sosyal bilimlerde içerik analizi teknikler ve örnek çalışmalar.* İkinci Baskı. Siyasal.

Bin Abbas, M.F., & Srikanthan, T. (2017). Low-complexity signature-based malware detection for IOT devices. In *International Conference on Applications and Techniques in Information Security,* (pp.181-189), Springer.

Blanchard, A. & Henle, C. (2008). Correlates of different forms of cyberloafing: The Role of norms and external locus of control. *Computers in Human Behavior, 24(3),* 1067-1084.

Bozeman, D. P., & Kacmar, K.M. (1997). A Cybernetic model of impression management processes in organisations. *Organisational Behaviour and Human Decision Processes, 69(1),* 9-30.

Brody, R.G., Mulig, E., & Kimball, V. (2007). Phishing, pharming and identity theft. *Journal of Academy of Accounting and Financial Studies, 11,* 43-56.

Brown, D.S. (2016). Cryptocurrency and criminality. The Police Journal: Theory Practice and Principles, 89(4), 327-339. https://doi.org/10.1177/0032258x16658927

Brown, D. S., & Wang, T. (2008). Cyberethics: identifying the moral, legal and social issues of cybertechnology in k-12 classrooms. *College Teaching Methods & Styles Journal, 4(2),* 29-36.

Bulut, S. & Gündüz, S. (2012). Exploring violence in the context of Turkish culture and schools. S. R. Jimerson, A. B. Nickerson, M. J. Mayer, & M. J. Furlong (Eds.), (In.) *Handbook of School Violence and School Safety: International Research and Practice* (2nd Ed.) (pp.165-174), Routledge.

Canavan, J.E. (2001). *Fundamentals of network security.* London, UK, Artech House.

Carlin, D., Burgess, J., O'Kane, P., & Sezer S. (2020). You could be mine(d): The Rise of cryptojacking. *IEEE Security & Privacy, 2020(18),* 16-22. https://doi.org/10.1109/MSEC.2019.2920585

Carlin D, O'Kane P, Sezer S, & Burgess J. (2018). Detecting cryptomining using dynamic analysis. In: 2018 *16th Annual Conference on Privacy, Security and Trust (PST),* (pp.1-6), IEEE. https://doi.org/10.1109/pst.2018.8514167 (08.05.2023).

Cassidy, W., Faucher, C., & Jackson, M. (2013). Cyberbullying among youth: a comprehensive review of current international research and its implications and application to policy and practice, *School Psychology International, 34(6) 2013,* 575-612. https://doi.org/10.1177/0143034313479697

Castells, M. (2005). *Ağ toplumunun yükselişi, enformasyon çağı: ekonomi, toplum, kültür.* (çev. Ebru Kılıç). Birinci Cilt, İstanbul Bilgi Üniversitesi Yayınları.

Chickowski, E. (2022). Cryptojacking Explained: How To Prevent, Detect, and Recover From it. https://www.csoonline.com/article/564521/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html Accessed: 22.09.2023.

Clayton R. (2005). Insecure Real World Authentication Protocols (or why is phishing so profitable). http://www.cl.cam.ac.uk/users/rnc1/phishproto.pdf. Accessed: 21.09.2023.

Clynes, M. E., & Kline, N. S. (1960). Cyborgs and Space. *Astronautics,* September, 26-76.

Cutler, R. (1996). Technologies, relations, and selves. (In.) L. Strate, R. Jacobson, & S. Gibson (Eds.), *Communication and Cyberspace: Social Interaction in an Electronic Environment,* (pp.317-333), Hampton.

Çetin, B. A., & Ceyhan, A. A. (2014). Ergenlerin İnternet'te Kimlik Denemeleri ve Problemli İnternet Kullanım Davranışları. *The Turkish Journal on Addictions, 1(2),* 5-46.

Dashevskyi, S., Zhauniarovich, Y., Gadyatskaya, O., Pilgun, A., & Ouhssain, H. (2020). Dissecting android cryptocurrency miners. *ACM,* 2020, 191-202.

Do, C. T., Tran, N. H., Hong, C., Kamhoua, C.A., Kwiat, K. A., Blasch, E., Ren, S., Pissinou, N. & Iyengar, S. S. (2017). Game theory for cyber security and privacy. *ACM Computing Surveys, 50(2), Article 30, (May 2017),* 1-37. http://dx.doi.org/10.1145/3057268

Doss, A. F. (2020). *Cyber Privacy: Who Has Your Data And Why You Should Care.* (1st Ed.) Ben Bella Books Inc.

Duda, R.O., & Hart, P.E. (1973). *Bayes Decision Theory*. Chapter 2, Pattern Classification and Scene Analysis, 10-43, New York, John Wiley.

Erdur-Baker, Ö., Kavşut, F. (2007). Akran zorbalığının yeni yüzü: siber zorbalık cyber bullying: a new face of peer bullying. *Eurasian Journal of Educational Research, 27, 2007,* 31-42.

Ergün, E., & Altun, A. (2012). Öğrenci gözüyle siber aylaklık ve nedenleri. *Eğitim Teknolojisi Kuram ve Uygulama, 2(1), 2012,* 36-53.

Erkoç, M. F. (2018). Güvenli internet kullanımı, *Bilişim Teknolojileri,* (İçinde) Serdar Bahadır Kert, (Ed.), (s.399-422), Nobel Yayın Dağıtım,

Ferrante, A., Malek, M., Martinelli, F., Mercaldo, F., & Milosevic, J. (2017). Extinguishing ransomware-a hybrid approach to android ransomware detection. In *International Symposium on Foundations and Practice of Security*, (pp. 242-258), Springer, Cham. https://doi.org/10.1007/978-3-319-75650-9_16

Fette, I., Sadeh, N., Tomasic, A. (2007). Learning to detect Phishing emails. In *Proceedings of the 16th International Conference on World Wide Web (WWW), ACM,* May 2007, (pp.649-656), Banff, Canada.

Fielder, A., König, S., Panaousis, E., Schauer, S., & Rass, S. (2018). Risk Assessment Uncertainties in Cybersecurity Investments. *Games* 2018, *9*, 34. https://doi.org/10.3390/g9020034

Garrett, R.K. & Danziger, J.N. (2008). On Cyberslacking: workplace status and personal internet use at work, *Cyberpsychology & Behaviour, (11)3,* 287-292.

Gibson, W. (1984). *Neuromancer.* Penguin Putnam Inc.

Gomez-Hernandez, J.A., Alvarez-Gonzalez, L., & García-Teodoro, P. (2018). R-Locker: Thwarting ransomware action through a honeyfile-based approach. *Computers & Security,* 73, 389-398. https://doi.org/10.1016/j.cose.2017.11.019

Goni, O. (2022), Cyber crime and its Classification, Int. J. of Electronics Engineering and Applications,10(1), 01-17, https://doi.org/10.30696/IJEEA.X.I.2021.01-17

Gökçe, O. (2006). *İçerik çözümlemesi kuramsal ve pratik bilgiler*. Siyasal Kitabevi.

Greene, M.B. (2006). Bullying in school: A Plea for measure of human rights. *Journal of Social Issues 62,* 63-69.

Gyöngyi, Z., Garcia-Molina, H., & Pedersen, J. (2004). Combating web spam with trustrank. In *Proceedings of The Thirtieth International Conference on Very Large Data Bases*, Volume 30, (pp.576–587), VLDB Endowment.

Haraway, D. (2006). *Siborg manifestosu: Geç yirminci yüzyılda bilim, teknoloji ve sosyalist-feminizm.* (Çev.) O. Akınhay. Agora Yayıncılık.

Herring, S. C. (2004). Content Analysis for New Media: Rethinking the Paradigm, *New Research for New Media: Innovative Research Methodologies Symposium Working Papers and Readings,* 47-66.

Hinduja, S., & Patchin, J.W. (2009). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying.* Carwin Press.

Hong, G., Yang, Z., Yang, S., Zhang, L., Nan, Y., Zhang, Z., Yang, M., Zhang, Y., Qian, Z., Duan, H. (2018). How you get shot in the back: A Systematical study about cryptojacking in the real world. In 2018 *ACM SIGSAC Conference on Computer and Communications Security (CCS '18),* (pp.1701-1713), ACM, NY, USA, 15-19 October 2018. https://doi.org/10.1145/3243734.3243840

Horan, C., & Saiedian, H. (2021). Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions. J. Cybersecur. Priv. 2021, 1, 580–596. https://doi.org/10.3390/jcp1040029

Hu, W., & Tan Y. (2017). Generating adversarial malware examples for black-box attacks based on GAN, arXiv:1702.05983, 1-7. https://doi.org/10.48550/arXiv.1702.05983

İşman, A. & Açmacı, N. (2021). Siber zorbalık kavramı üzerinden bir film incelemesi: Cyberbully (sanal zorbalık), *IETC-IDEC 21, IQC 21, ITEC 21, ISTEC 21, INTE 21, IWSC 21, ITICAM 21, Conference Paper,* (s.503-527).

Jindal, N., & Liu, B. (2008). Opinion spam and analysis. In *Proceedings of The International Conference on Web Search And Web Data Mining*, (pp.219-230), New York, ACM.

Kalaycı, E. (2010). Üniversite öğrencilerinin siber aylaklık davranışları ile öz düzenleme stratejileri arasındaki ilişkilerin incelenmesi, (Yayınlanmamış Yüksek Lisans Tezi), Hacettepe Üniversitesi Fen Bilimleri Enstitüsü.

Kara, I., & Aydos, M. (2022). The Rise of ransomware: Forensic analysis for Windows based ransomware attacks. *Expert Systems With Applications*, 190(2022), 1-14. https://doi.org/10.1016/j.eswa.2021.116198

Kaşıkçı, D. N., Çağıltay, K., Karakuş, T., Kurşun, E., & Ogan, C. (2014). Türkiye ve Avrupa'daki çocukların internet alışkanlıkları ve güvenli internet kullanımı, *Eğitim ve Bilim 2014, 39(171),* 230-243.

Kharraz, A. (2016). UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware, In *Proceedings of the 25th USENIX Security Symposium (USENIX Security 16),* (pp.757-772), USENIX Association.

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., Kirda, E. (2015). Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks, in *Detection of Intrusions and Malware, and Vulnerability Assessment, Vol. 9148 of Lecture Notes in Computer Science*, (pp.3-24), Springer International Publishing, Cham.

Kirda, E. (2017). UNVEIL: a large-scale, automated approach to Detecting ransomware (keynote). *In 2017 IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER),* (pp.1-1), IEEE. https://doi.org/ 10.1109/SANER.2017.7884603.

Kolukırık, S. & Gün, E. (2020). Bilişim teknolojilerinin suç eylemi üzerindeki etkisi: İnternet haberlerinde dijital suç örneği. *ZfWT* 12(3), (2020), 323-339.

Korkmaz, M., & Kıran-Esen, B. (2012). The Effects of peer-training about secure internet use on adolescents. *Turkish Psychological Counseling and Guidance Journal, 2012, 4(38),* 180-187.

Kowalski, R.M., Limber, S. P. & Agatston, P.W. (2012). *Cyberbullying: Bullying in the digital age.* Wiley & Blackwell.

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin, 140*(4), 1073-1137. https://doi.org/10.1037/a0035618

Krippendorff, K. (2013). C*ontent analysis: An Introduction to its methodology* (3.Ed.). Sage.

Krishnan, H.R., Saketh, S.Y., Vaibhav, V.T.M. (2015). Cryptocurrency mining-transition to cloud. *(IJACSA) International Journal of Advanced Computer Science and Applications, 6*(9), *2015,* 115-124.

Krueger, M. (1991). *Artificial reality II.* Addison-Wesley, Reading.

Kshetri, N., & Voas, J. (2022). Cryptojacking. Computer. *IEEE, Computer Society,* 55(1), 18-19. https://doi.org/10.1109/MC.2021.3122474

Kuehl, D.T. (2009). *From Cyberspace to Cyber-power: Defining the Problem, in Cyberpower and National Security*, ed. by F.D. Kramer, S. Starr, L.K. Wentz, National Defense University Press, Washington (D.C.).

Kut, S. (2013). Sibertektonik mekân. (Yayımlanmamış Doktora Tezi). İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü.

Lacey, B. (2007). Social aggression: a study of internet harassment. (Unpublished Doctoral Dissertation), Long Island University. New York, USA.

Lenhart, A. (2007). Cyberbullying and online teens. http://www.pewinternet.org/pdfs/PIP%20Cyberbullying%20Memo.pdf. Accessed:12.10.2023.

Levy, P. (1997). *Collective intelligence: Mankind's emerging world in cyberspace.* Perseus Books.

Li, F., Huang, M., Yang, Y., & Zhu, X. (2011) Learning to Identify Review Spam, DBLP Conference IJCAI 2011, January 2011, *Proceedings of the 22nd International Joint Conference on Artificial Intelligence*, 16-22, July 2011, (pp.2488-2493), Barcelona, Catalonia, Spain. https://doi.org/10.5591/978-1-57735-516-8/IJCAI11-414

Li, H., Zhou, S.Y., Yuan, W., Li, J., & Leung, H. (2020). Adversarial-example attacks toward android malware detection system. *Fellow, IEEE Systems Journal*, 14(1), March 2020, 653-656. https://doi.org/10.1109/JSYST.2019.2906120

Li, Q. (2006). Cyberbullying in Schools: A Research of Gender Differences. *School Psychology International. 2006; 27(2),*157-170. https://doi.org/10.1177/0143034306064547

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A Theoretical perspective. *MIS Quarterly,* 33(1), 71-90.

Lim, V.K., & Chen, D.J. (2012). Cyberloafing at the workplace: Gain or drain on work? *Behaviour & Information Technology, 31(4),* 343-353.

Lippert, K.J., & Cloutier, R. (2021). Cyberspace: A Digital Ecosystem. Systems 2021, 9-48. https://doi.org/10.3390/systems9030048

Little, D., Shinder, J., & Cross, M. (2008). *Scene of the cybercrime*. New York, USA, Elsevier.

Martin, K.A & Leary, M.R. (1999). Would you drink after a stranger? the influence of self-presentational motives on willingness to take a health risk. *Personality & Social Psychology Bulletin, 25(9),* 1092-1111.

McCombs, R., Barnes, J., Sood, K., & Barton, I. (2018). Wannamine Cryptomining: Harmless Nuisance or Disruptive Threat? https://www.crowds-trike.com/blog/cryptomining-harmless-nuisance-disruptive-threat Accessed: 21.04.2023.

McLuhan, M. (1964). Understanding media: The Extensions of man. McGraw Hill.

Medin, B. (2018). Dijital kültür, dijital yerliler ve günümüzdeki yeni film seyir deneyimleri, *Erciyes İletişim Dergisi Akademia, 2018, 5(3),* 142-158.

Meland, P.H., Bayoumy, Y., & Sindre, G. (2020). The Ransomware-as-a-service economy within the darknet. *Computers & Security*, 92. 101762. https://doi.org/10.1016/j.cose.2020.101762

Messmer, E. (2023). Tech talk: Where'd it come from, anyway?, *Pc World: Business Cen*. https://www.pcworld.com/article/147698/tech.html Accessed: 14.08.2023.

Metin, O. & Karakaya, Ş. (2017). Jean Baudrillard perspektifinden sosyal medya analizi denemesi. *Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi, 19(2),* 109-121.

Mitchell, T.M. (1997). *Machine learning*. New York, USA, McGraw-Hill.

Monica, Z.P, & Lindskog, D. (2016). Experimental analysis of ransomware on Windows and android platforms: Evolution and characterization. *Procedia Computer Science,* December 2016, 94, 465-472.

Moore, T., & Clayton, R. (2007). Examining the impact of website take-down on Phishing. In *Proceedings of The Anti-Phishing Working Group's Annual Ecrime Researchers Summit*, (pp.1-13), ACM.

Mukhopadhyay, U., Skjellum, A., Hambolu, O., Oakley, J., Yu, L., Brooks, R. (2016). A Brief survey of Cryptocurrency systems. In *2016 14th Annual Conference on Privacy, Security and Trust (PST).* (pp.745-752), IEEE. https://doi.org/10.1109/PST.2016.7906988

Musch, M., Wressnegger, C., Johns, M., Rieck, K. (2019). Thieves in the browser: web-based cryptojacking in the wild, In *The 14th International Conference,* (pp.1-10), ACM.

Nagy, P., & Koles, B. (2014). The Digital transformation of human identity: Towards a conceptual model of virtual identity in virtual worlds. *Convergence, 20(3),* 276-292.

Nakamoto, S. (2008). Bitcoin: A Peer-To-Peer Electronic Cash System. 1-9, 2008. https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf Accessed: 11.06.2023.

Nindyati, O., & Nugraha, I.G.B.B. (2019). Detecting scam in online job vacancy using behavioral features extraction. *2019 International Conference on ICT for Smart Society (ICISS),* (pp.1-4), Bandung, Indonesia. https://doi.org/10.1109/ICISS48059.2019.8969842

Nowicki, J. M. (2020). Data Security: Recent K-12 Data Breaches Show that Students are Vulnerable to Harm, *GAO Reports, September 2020,* 1-22. https://www.gao.gov/assets/710/709463.pdf Accessed: 23.12.2023.

O'Kane, P., Sezer, S., & Carlin, D. (2018). Countering cyber threats for industrial applications: An automated approach for malware evasion detection and analysis". *Journal of Network and Computer Applications*, 7(5), 321-327. https://doi.org/10.1049/ntw2.v7.510.1049/iet-net.2017.0207

Özdemir, N. G. (2006). Sanal topluluklarda izlenimi yönetme. (Yayımlanmamış Yüksek Lisans Tezi), Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 179s.

Öztürk, G. (2013). *Dijital reklamcılık ve gençlik*. Beta Yayınları.

Peker, A, & Ekinci, E. (2016). Genel öz-yeterliğin siber zorbalıkla başa çıkma davranışları üzerindeki yordayıcı etkisi. *Uluslararası Türkçe Edebiyat Kültür Eğitim (TEKE) Dergisi, 5(4),* 2126-2140. https://dergipark.org.tr/tr/pub/teke/issue/26927/283128

Purkait, S. (2012). Phishing counter measures and their effectiveness literature review. *Information Management & Computer Security*, 20(5), 382-420. http://dx.doi.org/10.1108/09685221211286548

Pusey, P., & Sadera, W. A. (2012). Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference. *Journal of Digital Learning in Teacher Education, 28(2),* 82-88.

Qamar, A., Karim, A., & Chang, V. (2019). Mobile malware attacks: Review, taxonomy & future directions. *Future Generation Computer Systems*, 97(2019), 887-909. https://doi.org/10.1016/j.future.2019.03.007

Raad, M., Yeassen, N.M., Alam, G.M., Zaidan, B.B., & Zaidan, A.A. (2010). Impact of spam advertisement through e-mail: A Study to assess the influence of the anti-spam on the e-mail marketing. *African Journal of Business Management*, 4(11), 2362-2367.

Ralston, S. M. & Kirkwood, W. G. (1999). The Trouble with applicant impression management. *Journal of Business and Technical Communication, 13(2),* 190-207.

Rass, S., Schauer, S., König, S., & Zhu, Q. (2020). *Cyber-Security in Critical Infrastructures A Game-Theoretic Approach,* Springer, Cham, Switzerland.

Ray, I., & Poolsapassit, N. (2005). *Using Attack Trees to Identify Malicious Attacks from Authorized Insiders*. S. De Capitani di Vimercati et al. (Eds.), ESORICS 2005, LNCS 3679, (pp.231-246), Springer-Verlag, Berlin Heidelberg.

Razali, M.A., & Mohd, S.S. (2019). CMBlock: In-Browser detection and prevention cryptojacking tool using blacklist and behavior-based detection method. In Badioze Zaman, H., et al. *Advances in Visual Informatics, IVIC 2019*. Lecture Notes in Computer Science, Vol 11870. (pp.1-12), Springer, Cham. https://doi.org/10.1007/978-3-030-34032-2_36

Reshmi, T.R. (2021). Information security breaches due to ransomware attacks- A systematic literature review. *International Journal of Information Management Data Insights*, 1(2021), 1-10. https://doi.org/10.1016/j.jjimei.2021.100013

Rudd, E.M., Rozsa, A., Günther, M., Boult, T.E. (2017). A Survey of Stealth Malware Attacks, Mitigation Measures, and Steps Toward Autonomous Open World Solutions. *IEEE Communications Surveys & Tutorials, 19(2),* Second Quarter, 1145-1172.

Rüth, J., Zimmermann, T., Wolsing, K., & Hohlfeld, O. (2018). Digging into browser-based crypto mining. In: *Proceedings of the Internet Measurement Conference 2018,* (pp.70-76), ACM. https://doi.org/10.1145/3278532.3278539

Saad, M., Khormali, A., & Mohaisen, A. (2018). End-to-End analysis of in-browser cryptojacking, *arXiv: Cryptography and Security*, 1-15. https://doi.org/10.48550/arXiv.1809.02152

Sahami, M., Dumais, S., Heckerman, D., Horvitz, E. (1998). A Bayesian Approach to Filtering Junk E- Mail. In Learning for Text Categorization-Papers from the AAAI Workshop, Madison Wisconsin. AAAI Technical Report, WS-98-05, 55-62.

Sahoo, A.K., Sahoo, K.S., Tiwary, M. (2014). Signature based malware detection for unstructured data in Hadoop. In *International Conference on Advances in Electronics Computers and Communications*, (pp.1-6), IEEE.

Savage, K., Coogan, P., Lau, H. (2015). The Evolution of Ransomware. *Symantec Security Tech. Report Version 1.0-August 6*, Mountain View, CA, USA.

Sayar, K. (2002). Psikolojik mekân olarak siberalan. *Yeni Symposium 40(2).* 60-67.

Schneider, C.M., Moreira, A.A., Andrade, José, S. Jr., Havlin, S., & Herrmann, H.J. (2011). Mitigation of malicious attacks on networks. *PNAS,* March 8, 2011, 108(10), 3838-3841. https://dx.doi.org/10.1073/pnas.1009440108/-/DCSupplemental

Schroeder, K. (2002). Safe Internet Use. *The Education Digest; Nov. 2002; 68(3), ProQuest Central*, 70-73.

Schroeder, A., & Lattanner, M. (2014). Bullying in the Digital Age: A Critical Review and Meta-Analysis of Cyberbullying Research Among Youth. Psychological Bulletin.

Sharifi, M., Fink, E., & Carbonell, J.G. (2011). Smartnotes: Application of crowdsourcing to the detection of web threats. *Carnegie Mellon University. Journal Contribution, IEEE*, 1-2.

Shinde, R., Veeken, P., Schooten, S., Berg, J. (2016). Ransomware: Studying transfer and mitigation. *2016 International Conference on Computing, Analytics and Security Trends*, (CAST), 19-21 December 2016, (pp.90-95), IEEE.

Shusterman, R. (2000). *Performing live: Aesthetic alternatives for the ends of art.* Cornell University Press.

Sırakaya, M. & Seferoğlu, S. S. (2018). Çocukların çevrim-içi ortamlarda karşılaştıkları riskler ve güvenli internet kullanımı. B. Akkoyunlu, A. İşman ve H. F. Odabaşı (Ed). *Eğitim Teknolojileri Okumaları 2018, 12. Bölüm*, (s.185-202), Pegem Akademi.

Simpson, B. & Murphy, M. (2014). Cyber-privacy or cyber-surveillance? legal responses to fear in cyberspace. *Information & Communications Technology Law, 23(3),* 189-191. https://doi.org/10.1080/13600834.2014.978551

Siroski, M., & Honig, A. (2012). Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. San Francisco, CA, USA, No Starch Press,

Sittig, D.F, & Singh, H. (2016). A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks". *Appl Clin Inform* 7(2), 624-632. http://dx.doi.org/10.4338/ACI-2016-04-SOA-0064

Slonje, R., & Smith, P.K. (2008). Cyberbullying: Another main type of bullying? *Scandinavian Journal of Psychology, 49,* 147-154.

Slonje, R., Smith, P. K. & Frisén, A. (2013). The Nature of cyberbullying, and strategies for prevention, *Computers in Human Behavior, 29(2013),* 26-32.

Smith, P. K. (2011). Cyberbullying and cyber aggression, *Handbook of school violence and school safety: International research and practice* (2nd ed.). Jimerson, S.R., Nickerson, A.B., Mayer, M.J., & Furlong, M. J. (Eds.), Routledge. https://doi.org/10.4324/9780203841372

Srinivasan, C.R. (2017). Hobby hackers to billion-dollar industry: the evolution of ransomware, *Computer Fraud & Security*, 2017(11), 7-9. https://doi.org/10.1016/S1361-3723(17)30081-7

Statista (2023). Internet usage worldwide- Statistics & Facts. https://www.statista.com/topics/1145/internet-usage-worldwide/#statisticChapter

Statista (2024). Countries with the highest internet penetration rate as of April 2024 https://www.statista.com/statistics/227082/countries-with-the-highest-internet-penetration-rate/

Stratton, J. (2002). *Siberalan ve kültürün küreselleştirilmesi*. Mehmet Doğan (Çev.), Cogito Sayı: 30, Yapı Kredi Yayınları.

Suler, J. (1996). *The Psychology of cyberspace*. http://www.rider.edu/suler/psycyber/psycyber.html Accessed: 13.11. 2023

Şenel, S., Günaydın, S., Sarıtaş, M.T., & Çiğdem, H. (2019). Üniversite öğrencilerinin siber aylaklık seviyelerini yordayan faktörler. *Kastamonu Education Journal, 27(1),* 95-105. https://doi.org/10.24106/kefdergi.2376

Tailor, J.P., Patel, A.D. (2017). A Comprehensive survey: Ransomware attacks prevention, monitoring and damage control. *International Journal of Research and Scientific Innovation (IJRSI),* IV(VIS), June 2017, 116-121.

Taylor, P.J, Dargahi, T., Dehghantanha, A., Parizi, R.M., & Choo, K. (2019). A systematic literature review of blockchain cyber security. *Digital Commun. Netw.*, 154, 3-13.

Tedeschi, J.T.; Lindskold, S. & Rosenfeld, P. (1985) Introduction to Social Psychology, West Publishing.

Tekiner, E., Acar, A., Uluagac, A.S., Kirda, E., Selcuk, A.A. (2021). SoK: Cryptojacking malware. In *Proceedings of the 2021 IEEE European Symposium on Security and Privacy (EuroS P),* 6-10 September 2021, (pp.120-139), IEEE. https://dx.doi.org/10.1109/EuroSP51992.%202021.00019

The Sun. (2018). Illegal Bitcoin Mining Factory Sparks Massive Blaze Thanks to Overheating Computers Used to Create Cryptocurrency. https://www.thesun.co.uk/news/5538526/bitcoin-mining-factory-cryptocurrency-illegal-russia-fire-overheating-computers/ Accessed: 07.05.2023.

TIFO-Today I Found Out (2012). This Day in History: The First Mass Commercial Internet Spam Campaign is Launched. https://www.todayifoundout.com/index.php/2012/04/this-day-in-history-the-first-mass-commercial-internet-spam-campaign-is-launched/ Accessed: 15.05.2023.

Timisi, N. (2005). Sanallığın gerçekliği: internetin kimlik ve topluluk alanlarına girişi, M. Binark & B. Kılıçbay (Der.). *İnternet, Toplum, Kültür,* (s.89-106), Epos Yayınları.

Törenli, N. (2005). *Yeni medya, Yeni iletişim ortamı*. Bilim ve Sanat Yayınları.

Tuparova, D., & Mehandzhiyska, K. (2018). Online educational computer games related to topic internet safety, analysis of case studies. *Proceedings of the National Conference on Education and Research in the Information Society*. (pp.057-066), Scitepress.

Turkle, S. (1996). Parallel lives: working on identity in virtual space. (In.) D. Grodin & T. R. Lindlof (Eds.), *Constructing the self in a Mediated World*, (pp.156-175), Sage. https://doi.org/10.4135/9781483327488.N10

Ugrin, C. J., Pearson, M.J. & Odom, M.D. (2007). Profiling cyber-slackers in the workplace: demographic, cultural, and workplace factors, *Journal of Internet Commerce, 6(3),* 75-89.

Van Schaik, P. (2017). Risk perceptions of cyber-security and precautionary behavior. *Computers in Human Behavior*, *75*, 547-559.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H.R. (2011). Why do people get phished? Testing individual differences in Phishing vulnerability with in an integrated, information processing model. *Decision Support Systems,* 51(3), 576-586.

Venugopal, D., & Hu, G. (2008). Efficient signature based malware detection on mobile devices. *Mobile Information Systems,* 4(1), 33-49.

Vitak, J., Crouse, J. & LaRouse, R. (2011). Personal internet use at work: Understanding cyberslacking, *Computers in Human Behavior, 27*, 1751-1759. https://doi.org/10.1016/j.chb.2011.03.002

Willard, N. (2004). An educator's guide to cyberbullying and cyberthreats. http://cyberbully.org/docs/cbcteducator.pdf Accessed: 12.10.2023.

Wang, A.H. (2010). Don't follow me: Spam detection in Twitter. *2010 International Conference on Security and Cryptography (SECRYPT)*, (pp.1-10), Athens, Greece.

Wang, E. Shih-Tse (2019.) Effects of brand awareness and social norms on user-perceived cyber privacy risk. *International Journal of Electronic Commerce, 23(2),* 272-293. https://doi.org/10.1080/10864415.2018.1564553

Whitty, M.T., & Buchanan, T. (2012). The Online dating romance scam: A Serious crime. *CyberPsychology, Behavior, and Social Networking*, 15(3), 181-183. https://doi.org/10.1089/cyber.2011.0352

Wong-Lo, M., & Bullock, L. M. (2011). Digital aggression: Cyberworld meets school bullies. *Part of a Special Issue: Cyberbullying By: Preventing School Failure, 55(2),* 64-70. https://doi.org/10.1080/1045988X.2011.539429

Wu, C., Yao, W., Pan, W., Sun, G., Liu, J., & Wu, L. (2022). Secure control for cyber-physical systems under malicious attacks, in *IEEE Transactions on Control of Network Systems*, June 2022, 9(2), (pp.775-788), IEEE. https://dx.doi.org/10.1109/TCNS.2021.3094782

Wu, G., Greene, D., Smyth, B., & Cunningham, P. (2010). Distortion as a Validation Criterion in the Identification of Suspicious Reviews. Technical Report, UCD-CSI-2010-04, Dublin, Ireland, University College Dublin, 2010.

Xu, G., Dong, W., Xing, J., Lei, W., Liu, J., Gong, L., Feng, M., Zheng, X., & Liu, S. (2022). Delay-CJ: A novel cryptojacking covert attack method based on delayed strategy and its detection. *Digital Communications and Networks,* 1-11. https://doi.org/10.1016/j.dcan.2022.04.030

Xu, J.J. (2016). Are blockchains immune to all Malicious attacks?. *Financial Innovation,* 2(25),1-9. https://dx.doi.org/10.1186/s40854-016-0046-5

Yağcı, M. & Yüceler, A. (2016). Kavramsal boyutlarıyla sanal kaytarma. *International Journal of Social Sciences and Education Research, 2(2),* 531-540.

Yaman, E, & Peker, A. (2012). The perceptions of adolescents about cyberbullying and cybervictimization. *Gaziantep University Journal of Social Sciences, 11(3),* 819-833. https://dergipark.org.tr/tr/pub/jss/issue/24238/256940

Yang, A., Lu, C., Li, J., Huang, X., Ji, T., Li, X., & Sheng, Y. (2023). Application of meta-learning in cyberspace security: a survey, *Digital Communications and Networks,* 9(1), 2023,67-78. https://doi.org/10.1016/j.dcan.2022.03.007.

Yaşar, S. & Yurdugül, H. (2013). The Investigation of Relation Between Cyberloafing Activities and Cyberloafing Behaviors in Higher Education, *Procedia- Social and Behavioral Sciences, 83,* 600-604.

Yazgan, Ç. Ü. & Yıldırım, A. F. (2020). Üniversite gençliğinde internet bağımlılığı ve derslerde siber aylaklık davranışları, *Gençlik Araştırmaları Dergisi, Aralık 2020, 8 (Özel Sayı),* 5-23.

Yetimoğlu, B. (2022). Siber tehdit istihbaratıyla özgün tehdit aktörleri veri kümesi oluşturma ve sınıflandırma, Yüksek Lisans Tezi, Fırat Üniversitesi Fen Bilimleri Enstitüsü, Elazığ, 69s.

Yohanandhan, R.V., Elavarasan, R.M., Manoharan, P., Mihet-Popa, L. (2020). Cyber-Physical Power System (CPPS): A review on modeling, simulation, and analysis with cyber security applications. *IEEE Access*, 2020(8),151019-64.

Yoo, K.H., & Gretzel, U. (2009). Comparison of Deceptive and Truthful Travel Review. *Information and Communication Technologies in Tourism*, 1(1), 37-47.

Yüksel, E. (2019). Türkiye'de iletişim araştırmalarında içerik analizi uygulamaları, sorunlar ve çözüm önerileri, *International Euroasia Congress on Scientific Researches and Recent Trends-V, 16-19 DEC, 2019*, The Book of Full Texts Volume-II, Editors. Prof. Dr. Gülzar İbrahimova & Dr. Terane Nağiyeva ISBN 978-625-7029-51-3, (s.134-152), Bakü, Azerbaycan.

Zeng, A., & Liu, W. (2012). Enhancing network robustness against malicious attacks, *Physical Rev. E 85,* 1-7. https://dx.doi.org/10.1103/PhysRevE.85.066130

Zhang, X., Ma, H., & Tse, C.K. (2022a). Assessing the robustness of cyber-physical power systems by considering wide-area protection functions. *IEEE J Emerg Sel Top Circ Syst*, 12(1), 107-114.

Zhang, X., Liu, D., Tu, H., & Tse CK. (2022b). An integrated modeling framework for cascading failure study and robustness assessment of cyber-coupled power grids. *Reliability Engineering & System Safety*, 226, 108654.

Zheng, M., Sun, M., Lui, J.C.S. (2013). Droid analytics: A Signature based analytic system to collect, extract, analyze and associate android malware. *In IEEE Conference on Trust, Security and Privacy in Computing and Communications*, 2013.

Zimba, A., Wang, Z., Mulenga, M., Odongo, N.H. (2020). Crypto mining attacks in information systems: An emerging threat to cyber security. *Journal of Computer Information Systems,* 60(4), 297-308. https://doi.org/10.1080/08874417.2018.1477076

Zinderen, İ. E. (2020). Yeni medyada kimlik inşası: youtuber kimliğine ilişkin bir inceleme, *Erciyes İletişim Dergisi, Ocak/January 2020, 7(1),* 415-434. https://doi.org/10.17680/erciyesiletisim.650956