JMTPR
Journal of Management Theory and Practices Research

Journal of **M**anagement **T**heory and **P**ractices **R**esearch
Cilt/Volume :3 | Sayı/Issue: 1 | Haziran/June 2022

SİBER DÜNYANIN KARANLIK YÜZÜ: DEEPWEB VE DARKNET

Mustafa COŞAR[1]

Makale İlk Gönderim Tarihi / Recieved (First): 05.05.2021 **Makale Kabul Tarihi / Accepted:** 23.06.2022

Atıf/©: Coşar, M. (2022). Siber Dünyanın Karanlık Yüzü: Deepweb ve Darknet. Journal of Management Theory and Practices Research, 3(1), 58-71

Özet

Günlük hayatın ve iş süreçlerinin dijitalleştiği günümüz dünyasında siber kavramı hayatımıza tam anlamıyla yerleşmiş durumdadır. Siber dünya, iletişim ve sosyalleşme amacı ile ortaya çıkmış olsa da ticaretten üretime, sağlıktan eğitime artık pek çok faaliyetin dijital dönüşümünü barındırmaktadır. Ödeme yönteminin bile değiştiği ve dijital paranın kullanılmaya başlandığı bu ortamların sağlıklı bir şekilde çalışabilmesi için kurallarının, limitlerinin ve iyi bir yönetim anlayışının olması gerekmektedir. Çünkü bu ortamlarda tehdit unsurlarının ve risklerin arttığı, önlem alınmazsa da çok büyük zararların ortaya çıktığı bilinmektedir. Siber dünyada yasal işlerin yapıldığı gibi yasa dışı işlerinde yapıldığı alanlar oluşmuştur. Bu çalışmada, siber dünyanın karanlık yüzü olarak adlandırılan DeepWEB ve DarkNET kavramlarının neler olduğu, bu ortamlara nasıl erişildiği, bu ortamların neler içerdiği, boyutlarının neler olduğu ve ne tür tehditleri içerdiği anlatılmıştır. Ayrıca, internet kullanıcıları için siber dünyanın bu karanlık yüzüyle nasıl baş edilebileceği hakkında bilgiler paylaşılmıştır.

Anahtar Kelimeler: DeepWEB, DarkNET, Siber güvenlik, Siber tehdit, VPN, TOR..

THE DARK SIDE OF THE CYBER WORLD: DEEPWEB AND DARKNET

Citation /©: Coşar, M. (2022). Siber Dünyanın Karanlık Yüzü: Deepweb ve Darknet. Journal of Management Theory and Practices Research, 3(1), 58-71

Abstract

In today's world, where daily life and business processes are digitized, the concept of cyber is fully embedded in our lives. Although the cyber world has emerged with the aim of communication and socialization, it now includes the digital transformation of many activities from trade to production, from health to education. For these environments, where even the payment method has changed and digital money has begun to be used, to operate in a healthy way, it is necessary to have rules, limits, and a good management approach. Because it is known that threats and risks increase in these environments and even if precautions are not taken, great damages occur. In the cyber world, there are areas where illegal work is done as well as legal work. In this study, information about DeepWEB and DarkNET environments, which is called the dark side of the cyber world, is given. It is explained how these environments are accessed, what these environments contain, what their dimensions are and what kind of threats they contain. In addition, information on how to deal with this dark side of the cyber world was shared for internet users.

Keywords: DeepWEB, DarkNET, Cyber security, Cyber threat, VPN, TOR.

1 Dr. Öğr. Üyesi, Bilgisayar Mühendisliği, Hitit Üniversitesi, Çorum Türkiye, mustafacosar@hitit.edu.tr ORCID: 0000-0001-6482-4592

1. GİRİŞ

Günlük hayatta bilinen ve kolaylıkla erişilebilen internet ortamı, web tarayıcılarının eriştiği web sayfalarından ve arama motorları aracılığıyla listelenen web sayfalarından oluşmaktadır. Bu ortam internetin yalnızca küçük bir parçasını oluşturmaktadır. Peki, geri kalan ve büyük bir bölümünü oluşturan parça neresidir? Bu sorunun cevabı, derin (deep) ve karanlık (dark) kelimeleri ile adlandırılmaktadır. Bu derin ve karanlık internete DeepWEB ve DarkNET adı verilmektedir.

Siber dünyanın derin ve karanlık yüzü, dünyanın çeşitli noktalarında bilgisayarlar olarak konumlandırılmış ve farklı erişim yöntemleriyle bağlantı sağlanabilen ortamlar olarak tanımlanabilir. Bu ortamlara bilinen web tarayıcıları ve arama motorları tarafından erişilememektedir. Ancak, bilgisayarlarda ve bağlantılarda bazı ayarlar yaparak ve özel yazılımlar kurarak erişilebilmektedir. Bilgisayarların izinli olmayan sitelere ve ortamlara erişimini sağlayan özel ağ ayarları ve bu ağ üzerinden karanlık ortamlara erişim içinde özel bir tarayıcı kurmak gerekmektedir. Bu özel ağ yapısına Virtual Private Network adı verilirken en bilinen tarayıcı da Tor adını almaktadır.

Dark web siteleri bilinen ".com" veya ".co" gibi uzantılar yerine ".onion" ile biten uzantılar almaktadır. Ayrıca, karanlık web siteleri, genellikle hatırlanması imkânsız olan Tek Düzen Kaynak Bulucu (Uniform Resource Loader, URL) oluşturan şifreli bir adlandırma yapısı kullanırlar. Örneğin, Dream Market adlı popüler bir ticaret sitesi, "eajwlvm3z2lcca76.onion" şeklinde anlaşılması zor olan bir adresi kullanmaktadır (Guccione, 2021).

İnternetin karanlık dünyasında, tümü tek bir uç noktada veya ayrı ayrı noktalarda listelenmiş milyonlarca web sitesi, pazar yeri ve mesajlaşma platformları, dosyalar ve veriler yer almaktadır. Bu dünya içerisinde yararlı bilgilerin yanında zararlı bilgiler de olabilmektedir. Guccione'de (2021) DarkNET'in tümünün zararlı olmadığını, aynı zamanda yararlı aktiviteler içinde kullanılabileceğini vurgulamaktadır. Örneğin, bir satranç kulübüne veya "Tor'un Facebook'u" olarak tanımlanan BlackBook sosyal ağına katılım yapılabilir.

Tor erişim ağı yaklaşık 6 binden fazla düğümden oluşan bir ağ haline gelmiştir. Bu programın asıl amacı, internet üzerinde faaliyette bulunan kullanıcının gizliliğinin yanı sıra trafik bilgisinin izlenmeden ilerlemesini sağlamaktır (Wikipedia, 2022). Bu iletişim ortamı 1990'lı yıllarda ABD deniz kuvvetleri tarafından geliştirilerek internet erişiminin gizliliği ve güvenliği için kullanılmıştır. Ardından, 2003 yılında sivil kullanıma açılmıştır.

Dijital dünyada hızla artan veri miktarı, işletmelerin veri toplama kaynaklarını karanlık ağları da içerecek şekilde genişletmesine yardımcı olabilir. Bu ağın içeriğinin tümüyle zararlı ve gizli bilgileri içerdiği düşünülmemelidir. Kişiler, kurumlar ve ülkeler yüzey webde bulamadıkları içerikleri ve bilgileri deep ve dark bölgede bulabilirler. Anahtar kelime, konu ve içeriklerin karanlık webden bazı araçlarla çekilmesi mümkündür. Bu araçlar, önceden olası hasarı önlemek veya en aza indirmek için karanlık ağın en derin köşelerinden verileri çıkarabilirler. Bu sayede, siber saldırı ve/veya fiziksel saldırı gerçekleştirebilecek saldırganlar önceden belirlenebilir. Ayrıca, kişisel ve kamuya açık olmayan bilgilerin (Non-Public Information, NPI) sızdırılıp sızdırılmadığı buralardan öğrenilebilir.

Bu çalışmada, internetin bilinen ve bilinmeyen ortamları tanıtılırken, bu ortamlara nasıl erişilebileceğini açıklanmıştır. DeepWEB ve DarkNET olarak adlandırılan bu ortamların neler içerdiği ve boyutlarının nerelere vardığı sayısal bilgilerle ortaya konmaya çalışılmıştır. Ayrıca, bu tür ortamların getirebileceği fırsatlara ve risklere de değinilmiştir. Özellikle, bireysel ve kurumsal olarak tüm internet kullanıcılarını ilgilendiren bilgi gizliliği ve güvenliği kavramları DeepWEB ve DarkNET özelinde bir kez daha

vurgulanmıştır.

2. KAVRAMSAL ÇERÇEVE

Bu bölümde siber kavramı kapsamında adlandırılan siber, siber uzay, siber tehdit, siber saldırı ve siber güvenlik kavramlarına değinilmeye çalışılmıştır.

2.1. Siber

Siber kavramı ilk kez canlılar ve makinalar arasındaki iletişim disiplinini inceleyen sibernetik biliminin babası sayılan Louis Couffignal tarafından 1958 yılında ortaya atılmıştır (Yılmaz, 2017). Sibernetik kelime kökünden türetilen bu terim bilgisayar sistemleri tarafından geliştirilen sanal ortamlar için kullanılan bir anlam kazanmıştır.

2.2. Siber Uzay

Siber uzay kullanıcıların ve bilişim sistemlerinin bir araya gelerek oluşturduğu ağa verilen isimdir. Bu uzay içerisinde kullanıcılar, veriler, bilgisayarlar, yazılımlar ve diğer bağlantı sistemleri yer almaktadır. Özellikle son yıllarda mobil sistemlerin yaygınlaşmasıyla ortamdan bağımsız olarak bu ağa bağlanılabilmektedir. Devletlerin de dijital platformları desteklemesi ve hizmetlerini bu platformlara taşıması siber uzayın zamanla genişleyerek büyümesine yol açmaktadır. Akkaya'nın 2021 yılında yaptığı çalışmasında internet ortamının genişlemesinin sayısal büyüklüğünü ifade etmek için 2021 Ocak ayı ölçümlerinde dünyadaki internet kullanıcısı sayısının 316 milyon kişi artarak 4,7 milyar sayısına ulaştığını ve büyümenin yıllık %7,3 olduğunu ifade etmektedir. Statista'nın (2021) yaptığı bir araştırmaya göre, 2021 yılı itibariyle dünya çapında 1,88 milyar web sitesinin olduğunu ortaya koymaktadır. Bu rakamın sürekli arttığı varsayıldığında bu sayının 2 milyara yaklaştığı söylenebilir.

Siber uzayda bilgisayar donanım ve yazılım birimleriyle kullanıcılar arasında bir iletişim kurabildiği gibi donanımlarda kendi arasında iletişim kurabilir hale gelmiştir. Nesnelerin interneti (İnternet of Things, IoT) olarak ortaya çıkan ve birbirleriyle haberleşebilen tüm donanım sistemleri siber uzayın bir parçası haline gelmiştir. Bu yönüyle siber uzay günden güne genişleyerek kendi kurallarını, yaşam sistemini ve mimarisini oluşturmaktadır.

2.3. Siber Tehdit ve Siber Saldırı

Bilişim teknolojileri aracılığı ile siber uzay içerisinde bulunan bilgiye dönük yapılan her türlü istismar, zarar verme ve yok etme girişimleri sonucu oluşan duruma siber tehdit adı verilir (Grenberg, 2017). Bu tehdidin gerçekleşmesi durumuna ise siber saldırı adı verilmektedir. Siber tehdit ve saldırı dünya genelinde sistemlerin birbirlerine internet ağı ile bağlı olması nedeniyle kullanıcıları, bilgisayarları, sistemleri ve sunucuları hedef alan uluslararası bir kapsama sahiptir. Furnell'e (2002) göre siber ortamlarda tehdit içerebilen ve suç olarak tanımlanan faaliyetler; dolandırıcılık, bilgi hırsızlığı, telif hakkı ihlali, casusluk, sabotaj, bilgi kaynaklarını devre dışı bırakma ve hacking faaliyetleri olarak sıralanmıştır. Bunlara ek olarak kişilerin ve sistemlerin spekülasyonu ve manipülasyonu olarak adlandırılan sosyal mühendislik faaliyetleri de söylenebilir.

Günümüz dünyasında bilgisayar ve internet kullanımının yaş ortalamasının çocukluk dönemine kadar düştüğü bilinmektedir. Cengiz (2021) bir çalışmasında siber saldırgan profilinden birisi olan hacker'lığın yaş ortalamasının 14-21 yaşları arasında yoğunlaştığını belirtmektedir. Bu nedenle kullanıcılar hangi yaş aralığında olursa olsun bilerek ya da bilmeyerek siber tehditlere açık hale gelebilmektedir.

2.4. Siber Güvenlik

Siber uzayda bulunan bileşenlerin her birine yönelik oluşan siber tehditlere karşı alınabilecek önlemlerin tümüne siber güvenlik adı verilir. Siber tehdit genellikle bilgi kaynaklarını hedef aldığı için bu bilginin korunması ve gizliliğinin sağlanması için alınan kurallar ve eylemlerin tamamı güvenlik olarak adlandırılır.

Bilişim Teknolojileri Kurumu (BTK) siber güvenliği; siber uzayda kullanıcıların ve kurum-kuruluşların güvenliklerini sağlamak amacıyla kullanılan; araçlar, güvenlik politikaları, kılavuzlar, eğitimler, uygulamalar, güvenlik teminatları ve her türlü teknolojik yapılanma olarak tanımlamaktadır (BTK, 2009). Daha kapsamlı bir şekilde bakıldığında siber güvenlik kavramı savunma hamlelerinin yanı sıra proaktif önlemler alarak bir adım önde olmayı da kapsamaktadır. Bunun için sistemin zafiyetlerini tespit etmek için önceden testler yaparak risklerin belirlenmesi gerekir. Böylece tehdit önceden algılanarak ortadan kaldırılmalıdır.

2.5. DeepWEB

DeepWEB arama motorlarının indeksleyemediği verileri içeren bir ağ grubudur. Bu ağ içerisinde şifrelenmiş web siteleri olduğu için kullanıcılar servis sunanların bilgilerini göremediği gibi servis sunanlar da kullanıcıların bilgilerini göremezler. Örneğin, Berat (2022) blog sayfasında DeepWeb dışına çıkarılmış bir bağlantı linki olan The Hidden Wiki paylaşmıştır. Bu link incelendiğinde çeşitli konu başlıklarında listelenmiş çeşitli bilgiler yer almaktadır.

Moore ve Rid (2016), 2723 aktif yayında olan DeepWEB sitesinin içeriğini sınıflandırmışlardır. Bu araştırma sonucuna göre web sitelerinin %57'sinin yasa dışı materyal barındırdığı ortaya çıkmıştır. Bu çalışmaya benzer bir çalışmada, McGuires 2019 yılında yapmıştır. Bu çalışmada, bir kuruma zarar verebilecek DarkWeb listelerinin 2016'dan 2019'a kadar %20 oranında arttığını belirlemiştir. İçerik listelemelerinin sonucunda İşletmelere uyuşturucu satışı dışında zarar verebilecek içeriklerin %60 oranında olduğu ortaya çıkmıştır.

DeepWEB'in bilinen web tarayıcıları ile listelenebilen içeriklerinde genellikle, tıbbi kayıtlar, ücrete dayalı içerik, üyelik gerektiren web siteleri ve gizli kurumsal web sayfaları yer almaktadır. Bu sayfaların toplam internetteki web sayfalarının sadece %1'ler gibi bir oranı kapsadığı söylenebilir. Erişime açık olmayan ve özel yöntemlerle erişilebilen web sayfalarının oranı ise bazı tahminlere göre, tüm internetin %96'sı ile %99'u arasına denk gelmektedir.

2.6. DarkNET

DarkNET, DeepWEB 'in kasıtlı olarak gizlenmiş bir alt kümesidir. Bu kümeye erişebilmek için Tor ve VPN gibi özel yöntemler gerekmektedir. DarkNET'in gizli tarafında bulunan web sitelerinin koleksiyonuna ise DarkWeb adı verilmektedir. Bu ağ içerisinde McGuires'e (2018) göre, bir risk oluşturabilecek içerikler aşağıdaki gibi özetlenmeye çalışılmıştır.

- Kötü amaçlı yazılım, DoS saldırısı ve botnet'ler dahil olmak üzere network saldırı araçları,
- Uzaktan erişim Truva atları, tuş kaydediciler ve açıklardan yararlanarak uzaktan erişim araçları,
- Birey, kurum ve ülke bazlı siber bilgiler,
- Eğitim dahil olmak üzere destek hizmetlerine yönelik veriler,

- Kimlik bilgileri,
- E-dolandırıcılık örnekleri,
- Ödeme araçlarına yönelik saldırı araçları,
- Müşteri bilgileri,
- Askeri veriler,
- Finansal veriler,
- Fikri mülkiyet/ticari sırlar,
- Ortaya çıkan diğer tehdit unsurları.

Nazah vd., 2020 yılında yaptıkları çalışmalarında, DarkNET ortamında suç tehditlerinin bir listesini şu şekilde sınıflandırılmışlardır.

- İnsan kaçakçılığı ve seks ticareti
- Pornografi endüstrisi
- Suikastlar ve pazarlaması
- Yasal olmayan ilaç ve uyuşturucu ticareti
- Çocuk pornografisi
- Terörizm
- Siber silah ve çalınan verilerin ticareti
- Dijital para kullanarak döviz değişimi

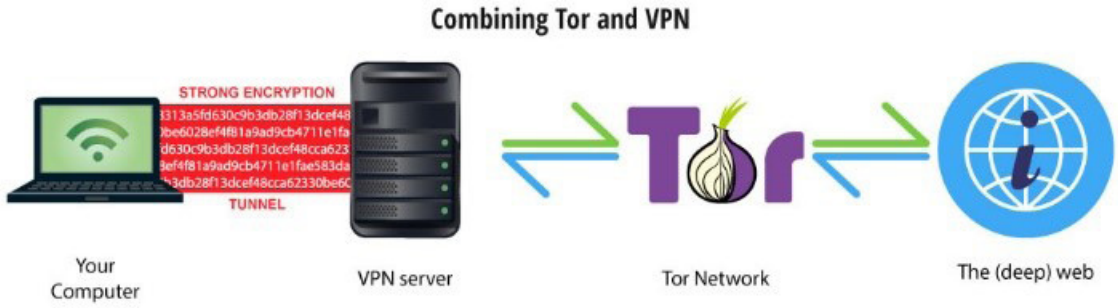
DarkNET, çeşitli elektronik veri transferinde mevcut olan hem metinsel hem de meta-veri içeriğinin analizi yoluyla, kullanıcı tarafından oluşturulan içeriğe (User Generated Content, UGC) gömülü olan güvenlik riskleri ve tehditleri ile ilgili bilgilerin istismarına ve analizine izin vermektedir (CyberSane, 2020).

2.7. TOR

The Onion Router (Soğan Yönlendirici) kelimelerinin kısaltması olan Tor, kullanıcıların internet trafiğini "kullanıcı bilgisayarları" üzerinden yönlendirmesine olanak tanıyan bir sistemdir. Bu sistem sayesinde trafik, kaynak kullanıcılara kadar izlenemediği için kullanıcı kimlikleri gizlenmiş olur (Demertzis vd., 2021). Tor, verileri bir katmandan başka bir katmana aktarmak için tüm dünyadaki tünelleri aracılığıyla bilgi taşıyan bilgisayarlarda "röleler" yaratmıştır. Şifrelenmiş bilgiler röleler arasına yerleştirilir. Tor trafiği bir bütün olarak üç röleden geçer ve daha sonra son varış noktasına iletilir (Yang vd., 2019). Bu mekanizma, düğümler ve Tor'un gizli servisleri arasında mükemmel bir ileri gizlilik sağlarken, aynı zamanda dünyanın dört bir yanındaki gönüllüler tarafından işletilen Tor düğümleri kendi aralarında uzlaşı aracılığıyla rutin olarak iletişim kurmuş olurlar.

İnternet kullanıcılarına sanal tünellerden oluşan bir yapı sunan ve onların gizliliklerini ve güvenlikleri sağlamaya yarayan Tor'un sağladığı en önemli özelliği kullanıcıların kimliklerini paylaşmadan bilgiye

erişme olanağı sunmasıdır. Tor'un kullanımında dikkat edilmesi gereken nokta ise internet trafik verilerinin şifrelenmemesi nedeniyle İnternet servis sağlayıcılar tarafından bu trafiğin izlenebilmesidir. Bunu engellemek için güvenli bir VPN ile kullanılması önerilmektedir. Bu yapı Şekil 1'de özetlenmeye çalışılmıştır.



Şekil 1. Tor network ve VPN'in bir arada kullanılması ile oluşan bağlantı mimarisi (Berat, 2022)

Şekil 1'deki mimariyi açıklamak gerekirse, kullanıcı bir VPN aracılığı ile bilgileri kriptolayıp Tor Browser bağlantısı üzerinden listelenen DeepWEB bilgisayarlara bağlantı sağlamış olur. Bu bağlantı sırasında çıkış yönlendiricilerinde bilgisayarlar hakkında bilgi toplamaya yönelik açıkların olabileceği söylenmektedir (McCoy vd., 2008).

Tor ağı yalnızca şifreleme sağlamakla kalmaz; aynı zamanda Güvenli Zengin Metin Transfer Protokolü (Hyper Text Transfer Protocol Secure, HTTPS) protokolünün normal trafiğini taklit etmek üzere tasarlanmıştır. Tor kanallarının algılanmasını deneyimli ağ mühendisleri veya analistleri için bile son derece karmaşık ve özel bir süreç haline getirmiştir. Spesifik olarak Tor ağı, HTTPS tarafından da kullanılan İletim Kontrol Protokolü (Transmission Control Protocol, TCP) bağlantı noktası 443'ü kullanabilir, bu nedenle yalnızca bağlantı noktası tarafından bir oturumu izlemek ve tanımlamak, bu tür trafiği belirlemek için güvenilir bir yöntem değildir (Pustokhina vd., 2020).

2.8. VPN

Özel Sanal Ağ (Virtual Private Network-VPN), iki bilgisayar arasında iletişimin güvenli ve tanımlı bir tünelden şifrelenerek yapılması yöntemidir. Bu tünel, ağ üzerinden bilgisayarların ilettiği verinin güvenliği için geliştirilmiştir. İki nokta arasında yapılan açık (şifrelenmemiş) veri alışverişi, verinin izlediği yol boyunca, aradaki ya da uç noktalardaki herhangi biri tarafından kolaylıkla görülebilir ve saldırı gerçekleştirilebilir.

Demir'e (2010) göre, ağlar üzerinde veri trafiğine yönelik saldırılar, dinleme (Eavesdropping) ve taraflardan birinin yerine geçme (Masquerading) saldırısı şeklinde gerçekleştirilebilir. Dinleme saldırısı, kötü niyetli bir kullanıcının, şifrelenmemiş veri iletişimini dinleyerek, kullanıcı adı ve şifre gibi gizli bilgileri fark ettirmeden alabilir. Ardından, gerçek kullanıcının eriştiği sistemlere bu bilgileri kullanarak erişebilir. Yerine geçme saldırısı ise, kötü niyetli kullanıcının kendisini, veri iletim yolunda gerçek sunucu ya da istemci gibi göstermek suretiyle saldırı gerçekleştirebilir. Bu tür saldırıların önüne geçmek için verinin şifrelenmesi ve/veya güvenli bir hattan iletilmesi gerekir. Bunu için VPN önerilmektedir. Erdurucan (2017), VPN'nin temel olarak verinin şifrelenmesi ve sarmalanması (encapsulation) ilkesine dayandığını vurgulamaktadır.

3. DarkNET ve DeepWEB 'in BOYUTLARI

Meland, Bayoumy ve Sindre (2020) DarkNET'i internetin düzensiz Vahşi Batısı olarak nitelendirmektedirler. DarkNET, siber suçluların güvenli bir şekilde iletişim kurduğu, bilgi ve diğer metaları paylaştıkları bir ortamdır. Dijital paranın çıkmasıyla ve ödeme aracı olarak kullanılmasıyla 2019 yılı itibariyle ticaret hacminin 1 milyar Amerikan doları olduğu tahmin edilmektedir.

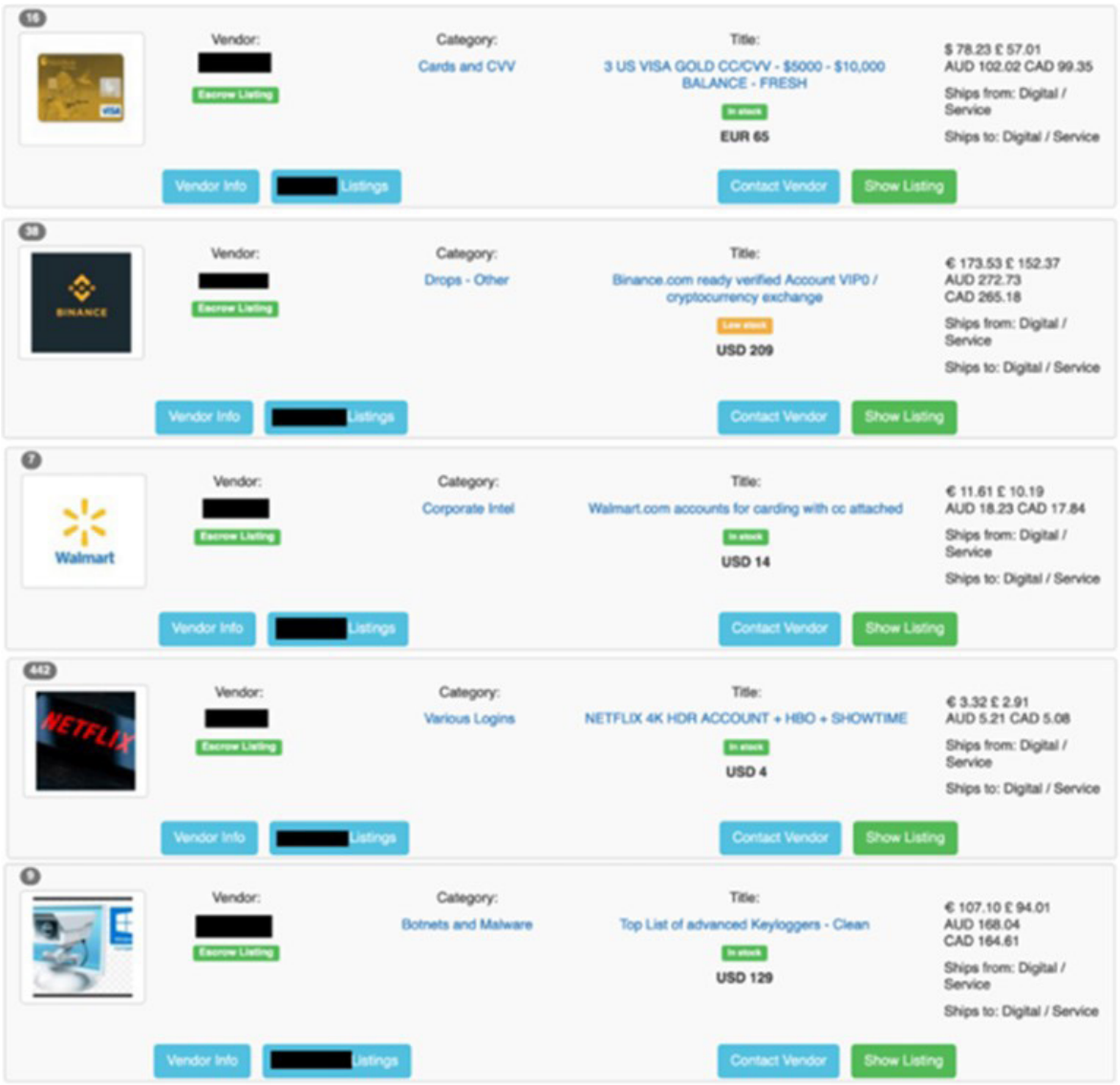
Karanlık ağın en büyük kaçak mal pazarı olan AlphaBay ortamı gizemli bir şekilde 2017 yılında çevrimdışı hale gelmiştir. Wall Street Journal üç ülkeyi kapsayan bir kolluk operasyonunun siteyi kapattığını, Kanada polisinin Quebec'teki sunucularına el koyduğunu ve ABD'li yetkililerin sözde yöneticilerinden biri olan Alexandre Cazes'in ABD'ye iadesini talep ettiğini bildirilmiştir. AlphaBay'in bir DarkNET pazarı için eşi benzeri görülmemiş büyüklüğüne işaret ederek, uyuşturucu, çalıntı kredi kartı ve diğer kaçak mal listesinin yaklaşık 300.000 sayısına ulaştığı raporlanmıştır. Bu ortamın günde 600.000$ ila 800.000$ arasında bir gelir getirdiği tahmin edilmektedir (Grenberg, 2017).

Bu ağ üzerinde bazı yasadışı işlemler için belirli aralıklarda bir ücret tarifesi bile oluşmuş durumdadır. Privacy Affair'in bu ağ içerisindeki işlem tarifelerinin bulunduğu Dark Web Price Index 2020 (Ignoffo ve Zoltan, 2021) raporunun 2021 yılında güncellenmiş hali Tablo 1' de listelenmiştir.

Tablo 1. DeepWEB tarafında açıklanan işlemler ve tarifeler listesi

Kategori	**Tarife**	**Ürün/Hizmet**	**Ort. Fiyat ($)**
Kredi kartı bilgileri	En az	Klonlanmış Visa, PIN numaralı Mastercard	25
	En çok	Kredi kartı bilgileri, harcama listeleri	240
Ödeme servisleri	En az	PayPal hesap bilgileri	30
	En çok	TransferGo bilgileri	510
Kripto hesap bilgileri	En az	Doğrulanmış Coinbase hesabı	610
	En çok	Doğrulanmış Kraken hesabı	810
Sosyal medya bilgileri	En az	Hack edilmiş Facebook hesabı	65
	En çok	Hack lenmiş Gmail hesabı	80
Hack'lenmiş Servisler	En az	Uber sürücü bilgileri	14
	En çok	Lykke hesabı	260
Sahte Dijital Belge Hazırlama	En az	Alberta CA sürücü belgesi	32
	En çok	Rus Pasaport bilgileri	100
Sahte Fiziksel Belge Hazırlama	En az	Sahte US Green Kart bilgileri	150
	En çok	Avrupa Birliği Pasaportları	4,000
E-posta Veri tabanı Dökümleri	En az	Sahte US Green Kart bilgileri	150
	En çok	USA Seçmen Veri tabanı	100
Zararlı Yazılım (Malware)	En az	Global düşük kalite, yavaş hız, düşük başarı oranı x 1000	50
	En çok	Avrupa için yeni yüksek kalite x 1000	2,500
Servis Dışı Bırakma DoS/DDoS Saldırısı	En az	Korumasız web sitesi, saniyede 10-50 bin istek, 1 saat	15
	En çok	Korumasız web sitesi, saniyede 10-50 bin istek, 1 ay	1,000

Tablo 1'de örnek bir işlem için en az ve en çok ücret karşılıkları verilmiştir. Bu liste her geçen gün yenilenmekte ve yeni işlemler ve yeni tarifeler eklenerek yeniden listelenmektedir. Ayrıca, bu raporda siber korsanlar tarafından ele geçirilen ve satışa sunulan kişisel ve kurumsal bilgilerin resimlerinden bazıları Şekil 2'de sunulmuştur.



Şekil 2. DeepWEB tarafında satışa sunulan bazı bilgiler

Kişisel ve kurumsal bilgilerin bazılarının belirli fiyatlarda satışa sunulduğu Şekil 2'de görülmektedir. Bu bilgiler arasında alış-veriş sitelerinin veri tabanı üyelik bilgileri, kredi kartı numarası ve şifresi, dijital paraların tutulduğu cüzdan gibi bilgiler yer almaktadır.

SONUÇ ve TARTIŞMA

Siber uzayın kişiler, kurumlar ve ülkeler tarafından görülen, bilinen, hesaplanabilen ve ölçülebilen boyutlarından tehdit ve saldırılar gelebilmektedir. Bilişim teknolojileri okuryazarlığının gelişmesi, gizlilik ve güvenlik konularındaki farkındalık düzeyinin artması ve bazı yeni teknolojik gelişmeler sayesinde bu tehdit ve saldırılara karşı koyabilecek bir duruma gelinebilmektedir. Ancak bilinemeyen, görülemeyen ve ölçülemeyen siber uzayın karanlık yüzünün ne tür tehditler ve riskler içerdiğini

bilmeden önlem almak zorlaşmaktadır. Bunun için tüm siber uzay bileşenleri hakkında bilinç düzeyinin geliştirilmesi, kavramların ve kapsamın çizilmesi, risk ve tehditlerin yönetilmesi gerekmektedir.

Bilgi, değeri kaybedilince anlaşılabilen bir varlık olduğu için kaybetmeden önce neler yapılması gerektiği bir yol haritası şeklinde hazırlanmalıdır. Kişilerin, kurumların ve devletlerin hayatta kalabilmesinin, rekabet edebilir olmasının ve dijital dünyanın gelişmelerine ayak uydurarak ilerleyebilmesinin tek yolu bilginin korunmasından geçmektedir.

Siber uzayın karanlık yüzü olarak bilinen DeepWEB ve DarkNET kavramlarının anlamı ve içeriğinin bilinmesi gizlilik ve güvenlik hakkında farkındalık yaratabilir. Ardından barındırdığı risk ve tehditlerin hesaplanabilen ve ölçülebilen taraflarının ortaya konması gerekir. Bir varlığı korumanın fiziki olarak sahip olunan silah sistemleriyle yeterli olmadığı, güç olgusunun bu tür önlemler ile sağlanamadığı bir çağda eğitim, altyapı ve vizyon değişikliklerinin zamanı geçmeden ele alınması önemli görülmektedir. Bu sayede risk ve tehditler fırsatlara dönüştürebilir.

Siber uzayın bir parçası olan insanın kendisini tam anlamıyla güvende hissedebilmesi için kişisel verilerinin güvende olduğunu ve bunların çeşitli yasal düzenlemelerle koruma altına alındığını bilmesi ön şart olmalıdır. Özellikle bireysellik, özgürlük ve demokrasi ortamının gelişmesi için siber uzayın bu karanlık boyutunda oluşan tehditlerin birer saldırı haline gelmeden önce bertaraf edilmesi güvenli ve sağlıklı bir toplum oluşturabilir.

Özellikle bireylerin olmasa da kurumların karanlık ağlardaki tehditleri sürekli olarak izlemesi gerekebilir. Bu izlemelerle tehditler tam olarak kontrol altına alınamasa da riskin boyutları hesaplanabilir. Sağlık, finans, eğitim, istihbarat ve askeri alanlar dahil olmak üzere farklı alanlarda siber faaliyetlerin ve tehditlerin sayısı arttıkça, bu tehditlerle baş edebilmek için kabiliyetlerin de geliştirilmesi gerektiği ortaya çıkmaktadır. İnsan kaynaklarının yetiştirilmesi, eğitilmesi, donanım ve yazılım sistemlerini üreterek ilk elden kontrol altına alınması, siber güvenlik farkındalık düzeyinin tüm toplum tarafında artırılması bu kabiliyetler arasında yer almaktadır.

Dark ve Deep tarafında nelerin olduğu hakkında bilgi sahibi olmak için bir haber sitesi olan Deep.Dot.Web (deepdot35wvmeyd5.onion/) adresine bakılabilir. Bu adrese Tor tarayıcı ile bağlanmak gerekir. Bu haber sitesinde bu ortamda yasadışı işlemler nedeniyle tutuklanan veya hapse atılan alıcıların bilgilerini bulmakta mümkündür. Moore ve Rid'e (2016) göre Tor üzerinde erişilen web sitelerinin %57'sinin uyuşturucu ve silah ticareti, cinayet ve çocuk pornografisi ile ilgili suç kapsamına giren faaliyetleri kolaylaştırdığı tahmin edilmektedir.

Siber dünyanın görünen ve görünemeyen taraflarında yaşarken siber güvenlik farkındalık düzeyinin artırılması için bireysel tarafta yapılabilecek bazı adımlar şu şekilde özetlenebilir.

- İnternet bağlantısı için herkese açık olan kablosuz internet Wi-Fi'den kaçınmak, zorunlu kalındığında ise kişisel bilgileri içeren iletişim yapmamak gerekir. Ayrıca, kafe, park, otel ve havaalanı gibi ortamlardan yapılan Wi-Fi ağlarının sağlayıcısının kimliğinden emin olarak kullanmak önemli görülmektedir.
- Banka işlemleri sırasında fiziki olarak kart kullanırken ATM cihazlarının kart yuvası, tuş takımları gibi donanımlarının aslına uygun olduğundan emin olunmalıdır. İnternet bankacılığı işlemlerinde ise banka web sayfasının gerçek olduğuna https protokolü ile servis verdiğine ve hatta https servisini dünya çapında güvenlik sağlayıcıları tarafından verildiğine emin olması gerekmektedir.
- Online ticaret, bankacılık ve ödeme sistemlerini kullanırken bilgilerin kaydedilmediğinden, üçüncü

taraf olarak banka doğrulama sistemlerinin varlığından emin olunmalıdır. Bu ortamlarda belirli bir limit ile işlem yapılmasına da dikkat edilmelidir.

- Eposta yoluyla gelen ve oltalama (phishing) olarak adlandırılan eposta tuzaklarına düşmemek için gönderen adresin doğruluğuna, içeriğin yapısına ve ilgisine bakılmalıdır. Ayrıca içerikte yer alan başka sitelere bağlantılara ve eklere dikkat edilmelidir.
- Kişisel ve hassas bilgilerin özenli bir şekilde korunmasına dikkat edilmelidir. Özellikle ortak kullanıma açık bilgisayar ortamlarında kişisel bilgilerin yazılmaması, saklanmaması ve paylaşılmamasına dikkat edilmelidir. Ayrıca bu bilgileri yazarken ekranların başkaları tarafından görünür olmasını engellemek gerekir.
- Donanım ve yazılım temini sırasında tanınır ve güvenilir markaların tercih edilmesi önemlidir. Ücretsiz, kırık ya da bilinmeyen yazılımları ve uygulamaları araştırmadan kullanmamak gerekir
- Dijital ortamların tümünde antivirüs ve güvenlik duvarı gibi güvenlik sistemlerini kullanmak ve sürekli güncel tutmak gerekir.
- Dijital ortamlara bağlanırken istenen doğrulama bilgilerini dikkatli bir şekilde belirlenmelidir. İlk aşama olan web sayfasının adreslerinin kontrolü iyi yapılmalıdır. Ardından kullanıcı adı ve parola zorluk derecesinin artırılmış olmasına dikkat edilmelidir. Kolay tahmin edilebilir veya kısa sürede çözülebilir parolalardan kaçınmak gerekir. Özellikle harf, sayı ve özel karakter içeren bir kombinasyona sahip olması sağlanmalıdır. İlk iki aşamayı sağlıklı bir şekilde geçtikten sonra doğrulama kodu gibi üçüncü bir güvenlik seviyesi isteyen sistemleri tercih etmek gerekir.
- Bilgi işlem merkezlerinde sistem günlüklerini ve ağ trafiğini analiz ederek tehdit ve saldırıların tespit edilmesi sağlanabilir. Kurumsal networklerde, ağ tabanlı, sunucu tabanlı, imza tabanlı, anomali tabanlı, spesifikasyon tabanlı, hibrit ve fiziksel saldırı tespit yöntemleri kullanılması önerilmektedir (Chaudhari ve Patil, 2017; Coşar ve Kıran, 2018; Coşar ve Arık, 2016). Ayrıca bilişim teknolojilerinin güncel kavramları olan yapay zekâ, makine öğrenme gibi alanlarından da yararlanılarak bu tehditlerin önceden belirlenmesi sağlanabilir (Umer vd., 2017).

Yukarıda maddeler halinde verilen hususlara ek olarak, internet tarayıcılarının mahremiyet ayarlarını iyi bir şekilde yapmak gerekir. Bunun için birçok tarayıcıda ortak olan mahremiyet sekmesinde, Private Browsing mode'u seçmek ve çerez (cookie) kullanmama gibi çeşitli ayarlar yapmak faydalı olabilir. Birçok yeni çevrimiçi davranışsal reklamcılık uygulamalarında Flash programının çerezleri kullanıldığından, bu yöntemle çevrimiçi takip edilmeyi engellemek çoğunlukla mümkün değildir (Karaarslan ve Eren, 2014). İnternet tarayıcıları eklenti yazılımları: DoNotTrackMe ve Ghostery gibi eklenti yazılımların devreye alınmasıyla sitelerin bilgi toplamasını engellemek mümkün olabilir.

Web sayfalarında suç teşkil edebilecek faaliyetlerin belirlenmesi ve suçluların bulunması aşamasında, kolluk güçleri, sosyal medya paylaşımları, Metasploit Decloaking Engine tarafından akıllı site indexleme aracı, Coin para trafiğinin izlenmesi, çeşitli algoritmalar yardımıyla Hash değeri analizi ile belge ve mesajların kaynağı gibi uzman yöntemler kullanmaktadırlar. Siber saldırganları yanıltmak için hazırlanan balküpü (Honeypot) gibi sistemleri konumlandırarak etkili bir savunma tercih edilebilir. DarkWeb pazar yerleri, siber suçluların yasa dışı suçlarını yaymaları ve yürütmeleri için ana platformlardan biridir. Bu nedenle, bu pazar yerlerindeki bilgileri önceden elde ederek, suçluları tespit etme ve yakalama aşamasında bir adım önde olunabilir (Nazah vd., 2020). Travis (2015) araştırmasında, finansal verileri satmak için anonim pazaryerlerinin ve forumların kullanılmasıyla İngiltere ve Galler'de yaklaşık 5,1

milyon çevrimiçi dolandırıcılık vakası belirlendiğini vurgulamaktadır.

Teknolojik gelişmelerin ve bilişim teknolojilerinin faydalarının ve zararlarının tüm yönleriyle ele alınarak bir kullanım politikası belirlenebilir. Torunlar (2018) çalışmasında yazılım ve donanım olarak teknolojik ürünlerin ve ağ sistemlerinin nasıl ve ne kadar kullanılacağının derinlemesine ele alınmasını önermektedir. Ayrıca, bu sistemlerin kar ve zararlarının hesaplaması yapılarak yaklaşılması gerektiğini söylemektedir.

Siber tehdit, siber suç, siber istihbarat ve siber güvenlik alanlarında bireylerin ve kurumların farkındalık düzeyleri geliştirilmelidir. Bilgisayar uzmanlarına ise siber saldırı ve savunma alanlarında bilgi ve tecrübelerini geliştirici eğitimler verilebilir. Ayrıca anlık ve dönemsel siber saldırı tatbikatları ile kurumların ve ülkelerin siber güçlerini artırmak önemli görülmektedir. Tuğal vd., (2021) bu konuda ilk atılacak adımların arasında, bilgisayar kullanıcılarına farkındalık eğitimlerinin verilmesini önermektedirler.

KAYNAKÇA

Akkaya, M. A. (2021). Bilgi Kaynağı ve Bilgiye Erişim Aracı Olarak İnternet Algısı: Kuşaklararası Yaklaşım Farklılığının Karşılaştırılması. Bilgi Yönetimi, Cilt 4, Sayı 2, ss.222-239, Doi:10.33721/by.947918

Berat, Y. (2022). Tor ve VPN ile Çevrimiçi Gizliliğinizi Artırın, Gizlilik ve Güvenlik Blog sayfası, İnternet Adresi: https://gizlilikveguvenlik.com/tor-vpn/, Erişim Tarihi: 18 Mayıs 2022.

BTK. (2009). Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınmasi Gereken Tedbirler, İnternet Adresi: https://www.btk.gov.tr/uploads/undefined/sg.pdf, Erişim Tarihi: 17 Mayıs 2022.

Cengiz, G. (2021). Siber Suçlar, Sosyal Medya ve Siber Etik. İletişim Çalışmaları Dergisi, Cilt 7, Sayı 3, 2021, ss.407-424, Doi: 10.17932/IAU.ICD.2015.006/icd_v07i3001

Chaudhari R. R. & Patil, S. P. (2017). Intrusion detection system: Classification techniques and datasets to implement, International Research Journal of Engineering and Technology (IRJET), Vol. 4, no. 2, Feb-2017.

Coşar M., Arık İ. (2016). The Importance of Traffic Analysis for Network Security. 1st International Conference on Engineering Technology And Applied Sciences, 21.04.2016.

Coşar, M. & Kıran, H.E. (2018). Rule-Based Performance Measurement in Open Source IDS Systems, International Conference on Advanced Technologies Computer Engineering and Science, 2018, 535-537.

CyberSane. (2020). DarkNet, European Union's Horizon 2020 Project, İnternet Adresi: https://www.cybersane-project.eu/system/darknet/, Erişim Tarihi: 20 Mayıs 2022.

Demertzis, K., Tsiknas, K., Takezis, D., Skianis, C., Iliadis, L. (2021). Darknet Traffic Big-Data Analysis and Network Management for Real-Time Automating of the Malicious Intent Detection Process by a Weight Agnostic Neural Networks Framework, Electronics 2021, Vol.10 (7), 781, Doi:10.3390/electronics10070781

Demir, F. (2010). Güvenli Veri İletiminde Kullanılan VPN Tiplerinin Uygulaması ve Performans Analizi, Yayımlanmamış Yüsek Lisans Tezi, İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü, 2010.

Erdurucan, S. (2017). İnternet Medyasında Gizli Belge Yayıncılığının Teknik ve Elektronik Analizi: Wikileaks ve Panama Belgeleri, Yayımlanmamış Yüsek Lisans Tezi, Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü, 2017.

Furnell, S. (2002). Cybercrime: Vandalizing The Information Society. Addison-Wesley. London, 2002.

Greenberg, A. (2017). The Biggest Dark Web Takedown Yet Sends Black Markets Reeling, JUL 14, 2017, İnternet Adresi: https://www.wired.com/story/alphabay-takedown-dark-web-chaos/, Erişim Tarihi: 20 Mayıs 2022.

Guccione, D. (2021). What is the dark web? How to access it and what you'll find, 2021, CSO SPOTLIGHT: DARK WEB, İnternet Adresi: https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html

Ignoffo, Z. & Zoltan, M. (2021). Dark Web Price Index 2021, İnternet Adresi: https://www.privacyaffairs.com/dark-web-price-index-2021/, Erişim Tarihi: 10 Mayıs 2022.

Karaarslan, E. & Eren, M.B., Koç, S. (2014). Çevrimiçi Mahremiyet: Teknik ve Hukuksal Durum İncelemesi, Türkiye'de İnternet Konferansları (inet-tr'14), Kasım 2014, İnternet Adresi: https://www.researchgate.net/publication/271762529_Cevrimici_Mahremiyet_Teknik_ve_Hukuksal_Durum_Incelemesi_Online_Privacy_Technical_and_Forensic_Case_Study, Erişim Tarihi: 10 Mayıs 2022.

McCoy, D., Bauer, K., Grunwald, D., Kohno, T., Sicker, D. (2008). Shining light in dark places: Understanding the Tor network, Privacy Enhancing Technologies, Springer Berlin Heidelberg, 2008, Doi:10.1007/978-3-540-70630-4_5.

McGuire, M. (2018). Into The Web of Profit-2018, İnternet Adresi: https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf, Erişim Tarihi: 12 Mayıs 2022.

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

Moore D. & Rid T. (2016). Cryptopolitik and the Darknet, Survival, Global Politics and Strategy, Volume 58, 2016, Issue 158:1, 7-38, Doi:10.1080/00396338.2016.1142085.

Nazah, S., Huda, S., Abawajy J., Hassan, M. M. (2020). Evolution of Dark Web Threat Analysis and Detection: A Systematic Approach, IEEE Access, vol. 8, pp.171796-171819, 2020, Doi:10.1109/ACCESS.2020.3024198.

Pustokhina, I., Pustokhin, D., Gupta, D., Khanna, A., Shankar, D., Nhu, N. (2020). An Effective Training Scheme for Deep Neural Network in Edge Computing Enabled Internet of Medical Things (IoMT) Systems, IEEE Access, 2020, Vol.8, Page(s):107112-107123, Doi:10.1109/ACCESS.2020.3000322.

Statista. (2021). How Many Websites Are There?. İnternet Adresi: https://www.statista.com/chart/19058/number-of-websites-online/, Erişim Tarih: 10 Nisan 2022.

Torunlar, M. (2018). Ulusal Bilgi/Veri Politikalarının Yeni Rota Sorunu: Tekinsiz Vadi' de Yol Almak. Bilgi Yönetimi, Cilt 1, Sayı 2, ss.119-133, Doi: 10.33721/by.486164

Travis, A. (2015). Crime rate in England and Wales Soars as Cybercrime is Included for First Time, The Guardian, Oct. 2015, İnternet Adresi: https://www.theguardian.com/uk-news/2015/oct/15/rate-in-england-and-wales-soars-as-cybercrime-included-for-first-time, Erişim Tarihi: 15 Mayıs 2022.

Tuğal, İ., Almaz, C. & Sevi, M. (2021). Üniversitelerdeki Siber Güvenlik Sorunları ve Farkındalık Eğitimleri, Bilişim Teknolojileri Dergisi, Cilt.14, Sayı.3, ss.229-238, Temmuz 2021, Doi:10.17671/gazibtd.754458.

Umer, M. F., Sher M. & Bi, Y. (2017). Flow-based intrusion detection: Techniques and challenges, Computer Security, vol. 70, pp. 238-254, Sep. 2017.

Wikipedia. (2022, Jan 7). Tor (network), İnternet Adresi: https://en.wikipedia.org/wiki/Tor_(network), Erişim Tarihi: 14 Mayıs 2022.

Yang, Y., Yu, H., Yang, L., Yang, M., Chen, L., Zhu, G., Wen, L. (2019). Hadoop-based Dark Web Threat Intelligence Analysis Framework, In Proceedings of the 2019 IEEE 3rd Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), Chongqing, China, 11-13 October 2019, pp.1088-1091.

Yılmaz, O. (2017). Küreselleşme Sürecinde Dönüşen Güvenlik Algısı ve Siber Güvenlik, Cyberpolitik Journal, Yıl 2017, Cilt 2, Sayı 4, sayfa 22-43.