İLETİŞİM TEKNOLOJİLERİNİN WEB SALDIRILARINDA KULLANIMI VE HACKER ETİKETLEMESİ: ZONE-H MODELİNİN ANALİZİ

Mustafa AYDEMİR
Dr, İletişim Fakültesi, Ege Üniversitesi, İzmir/Türkiye, 0000-0001-9414-4053
dr.mustafa.aydemir@gmail.com

ÖZET

Dijital dünyada veri güvenliği konusunda yaşanan çeşitli sorunlar içerisinde web tabanlı siber saldırılar büyük bir tehdit oluşturmaktadır. Web servisleri üzerinde gerçekleştirilen veri hırsızlığına karşı yönetim organları tarafından çeşitli önlemler alınmaktadır. Yazılım ve donanım tabanlı koruyucu uygulamalar yanında küresel ölçekteki hukuki düzenlemeler etkin çözüm politikaları arasında yer almaktadır. Siyah şapkalı hacker olarak tanımlanan özneler, web servislerine yönelik saldırılarını izleme periyodunda etiketleyerek yayınlamaktadır. Bu etiketleme sisteminin dijital ortamda etik düzeyde kanıtlanması aşamasında gerçek zamanlı siber saldırıları izleyen ve etiketleyen tek resmi platform olarak Zone-H kullanılmaktadır. Bu çalışma kapsamında 1-31 Ekim 2022 döneminde Zone-H sistemi üzerinde bir aylık saldırı analizi yapılmıştır. Analiz sürecinde 968 saldırı saptanmış olup, bu saldırıların 9 farklı işletim sistemi üzerinden yapıldığı tespit edilmiştir. Saldırılar bölgesel olarak sınıflandırıldığında Asya kıtası 354 saldırı ve %36,5 ile ilk sırada yer almaktadır. Ülke bazında ise Endonezya 250 saldırı ile ilk sırada yer almaktadır. Kuzey Amerika 198 saldırı ve %20,45 ile ikinci sırada yer alırken ABD 172 saldırı ile bölge ülkeleri arasında ilk sıradadır. Avrupa kıtası ise 129 toplam saldırı ve %13,32 ile üçüncü sırada bulunmaktadır. Türkiye'nin bu grup içerisinde 62 saldırı ile ilk sırada olduğu görülmektedir. Güney Amerika toplam 116 saldırı ve %11,98 ile dördüncü sırada olup, Brezilya 66 saldırı ile ülke bazında ilk sırada bulunmaktadır. Afrika kıtası 36 saldırı ve %3,71 ile dördüncü sırada yer almaktadır. Çalışmada, web servis saldırılarını gerçekleştiren kişi ve grupların eylemlerinin çevre ülkelerden merkez ülkelerin sistemlerine doğru yönelim gösterdikleri anlaşılmaktadır.

Anahtar Kelimeler: Zone-H, Web Servis Saldırısı, İletişim Teknolojileri, Yasadışı Etiketleme, Avrupa Konseyi.

The Use of Communication Technologies in Web Attacks and Hacker Tagging: Analysis of the Zone-H Model

ABSTRACT

Web-based cyber-attacks pose a major threat among the various problems experienced in data security in the digital world. Various measures are taken by governing bodies against data theft on web services. In addition to software and hardware-based protective applications, legal regulations on a global scale are among the effective solution policies. Subjects defined as black hat hackers label and publish their attacks on web services during the monitoring period. Zone-H is used as the only official platform that monitors and labels real-time cyber attacks in order to prove this labeling system at an ethical level in the digital environment. Within the scope of this study, a one-month attack analysis was conducted on the Zone-H system during the period October 1-31, 2022. During the analysis process, 968 attacks were detected and it was determined that these attacks were made over 9 different operating systems. When the attacks are classified regionally; Asia ranks first with 354 attacks and 36.5%. On a country basis, Indonesia ranks first with 250 attacks. North America ranks second with 198 attacks and 20.45%, while the USA ranks first among the countries in the region with 172 attacks. Europe ranks third with 129 total attacks and 13.32%. Turkey ranks first in this group with 62 attacks. South America ranks fourth with 116 total attacks and 11.98%, with Brazil ranking first in terms of countries with 66 attacks. Africa ranks fourth with 36 attacks and 3.71%. In the study, it is understood that the actions of individuals and groups who carry out web service attacks are directed from peripheral countries towards the systems of central countries.

Keywords: Zone-H, Web Service Attack, Communication Technologies, Hacker Tagging, Council of Europe.

1. GİRİŞ

Büyük hacimli hassas veriler ve web sitelerindeki güvenlik açıklıkları nedeniyle bu uygulamalara yönelik saldırıların sayısı önemli ölçüde artmaktadır. Web sitelerine yapılan saldırıların farklı amaçları vardır, bunlardan biri de yetkisiz değişikliklerin yapılmasıdır [1]. Web site saldırıları web ve sayfa içeriğini ya da sistem dosyalarını değiştirmek için bir web sitesine izinsiz girmeyi içeren siber suçtur. Holt'a göre; tahrifatlar (İng. Defacement), "bilgisayar korsanlarının bakış açılarını ve inançlarını gösteren mesajlar ve resimler yayınlamalarına ve isimlerini ve grup bağlantılarını listeleyerek statü kazanmalarına olanak tanımaktadır" [2]. Bu saldırı yapısı, bir web sitesine yapılan ve tüm sitenin ya da bir veya daha fazla web sayfasının görsel görünümünü değiştiren bir saldırı olarak verilen tanıma ek olarak kimi zaman "hacktivizm" şeklinde kabul edilmekte ve bazı sosyal ağ araçlarına karşı yapılan kısıtlamaları da kapsamaktadır [3].

Web saldırıları; imza tabanlı tespit ve anomali tabanlı tespit olarak iki yaklaşımla değerlendirilebilir. İmza tabanlı tespit, kötü niyetli yüklerin özellikleri hakkında bilgi içeren bir veritabanı aracılığıyla saldırıları değerlendirmeyi amaçlamaktadır [4]. Web saldırıları temelde bir web sitesinin içeriğinin veya görünümünün bir saldırgan tarafından izinsiz olarak değiştirilmesidir. Bu tür saldırılar bilgisayar ağları ve web uygulamaları üzerinde gerçekleştirilen kötü niyetli eylemleri ifade etmektedir. Web saldırıları, web uygulamalarının ve sunucularının güvenlik açıklarından yararlanarak yetkisiz erişim sağlama, bilgi hırsızlığı, veri değiştirme veya hizmet kesintisi gibi zararlı faaliyetler içermektedir. Bu tür eylemler kuşkusuz siber güvenliği ihlal ederek kullanıcıların verilerini ve gizliliklerini tehlikeye atabilir ve kurumların itibarını ve iş sürekliliğini etkileyebilmektedir. Web saldırıları aynı zamanda web sitesi operasyonlarını kesintiye uğratmak, sahibinin itibarına zarar vermek ve potansiyel veri kayıplarına neden olmak gibi çeşitli riskler barındırmaktadır [5]. Web tahrifatının kendisi veri çalmak veya önemli bir hasara neden olmakla birlikte genellikle daha büyük bir "siber suç" [6-7-8-9-10-11-12] operasyonunun da göstergesidir.

Siber suç kavramını bilinç düzeyinde ele alarak "başkaları için olumsuz sonuçlar doğurması amaçlanan çevrimiçi faaliyetler [13] şeklinde tanımlayan Kirwan ve Power, aynı zamanda bu suçları tipolojik olarak sınıflandırma yoluna giderek "İnternet destekli suçlar, İnternete özgü suçlar ve Sanal dünyalarda işlenen suçlar" [14] şeklinde üç temel siber suç tipolojisinin ana hatlarını da çizmektedir. Siber suç konusunu, siber teknoloji ile ilişkilendiren Aiken vd., [15] ileriye dönük olarak bir suçun belli belirsiz de olsa bir noktada siber teknolojileri içermesi halinde "siber suç" olarak etiketlenebileceği ve gözlemlenebileceğini ileri sürmektedir.

Web saldırılarına karşı mücadele etmek için güvenlik önlemleri, web uygulamalarının düzgün bir şekilde yapılandırılması, düzenli güncelleme ve güvenlik açıklarının düzeltilmesi gibi adımların atılması kişisel çabalardan ziyade saldırıların yoğun olarak yapıldığı kurumsal hesaplar üzerinden gerçekleştiğinden kurumsal politikalar ve teknolojik altyapı ve teknik destek birimlerinin niteliği de önem kazanmaktadır. Bilişim alanı çevrimdışı bağlantılar ile çalışmakla birlikte genel olarak çevrimiçi sistemler ile çalışmaktadır. Bu bağlamda Siberuzam alanı en temelde web tabanlı sistemler üzerinden internet mecralarında inşa edilmektedir. Bu durumda ortaya çıkan tahrifatlar, internet bağlantılı web uygulamaları ile bağlantılı siteler üzerinden direkt ya da dolaylı olarak gerçekleşmektedir.

Bazı durumlarda web tahrifatı, hassas bilgilerin çalınması veya web sitesi ziyaretçilerinin bilgisayarlarına kötü amaçlı yazılım yüklenmesi gibi daha kötü niyetli faaliyetler için bir kılıf olarak kullanılır. Siber suç alanına giren bu çalışmalarda "gömülü zararlı dosya yüklemesi" [16-17] ön plana çıkmaktadır. Bir web sitesini tahrif etmek, saldırganlar için bilgisayar korsanlığı becerilerini göstermenin veya siyasi bir açıklama yapmanın bir yolu da olabilir. Bu noktada gerek siyasi gerekse

ekonomik olası zararlara karşı yöneticilerin nitelikli çözümler üretmesi ve itibara yönelik zararları azaltması da beklenmektedir [18]. Bazı durumlarda web saldırıları konusunda tercih edilen "script kiddie" [19] yöntemi, düşük seviyeli ve bağlantılı bir saldırı türü web tahrifatı şeklinde kabul edilmekte ve kullanılabilmektedir. Web tahrifatında bu konu dışında da çeşitli uygulama örnekleri yer almaktadır.

Genel olarak web tahrifatı, küçük bir sorun gibi görünse de daha ciddi siber suç faaliyetleri için önemli bir soruna karşılık gelmektedir. Web sitesi sahipleri web tahrifatını ciddiye almalı ve daha fazla zararı önlemek için sitelerindeki yetkisiz değişiklikleri araştırmalıdır. Bir kuruluşun web sitesinin tahrif edilmesi, izinsiz değişiklik keşfedilip düzeltilene kadar ziyaretçileri yanıltıcı bilgilere maruz bırakır. Web tahrifatı, çevrimiçi bir varlık geliştiren işletmeler için önemli ve büyük bir tehdittir [20]. Web servis saldırılarının izlenmesi ve etiketlenmesi, siber güvenlik uzmanlarının ve savunma ekiplerinin saldırıları daha iyi anlamaları ve etkili önlemler almaları için önemli bir adımdır. Bu izleme politikası; erken tehdit tespiti, veri güvenliğini sağlama, şüpheli etkinliklerin denetimi, saldırıların sınıflandırılması, saldırı önleme ve savunma ile yasal ve hukuki süreçlerin etkin bir biçimde yürütülmesini de sağlayabilmektedir.

Web tahrifatı konusunda en yaygın kullanıma sahip saldırılar arasında yer alan Dağıtılmış Hizmet Engelleme (DDoS) saldırıları, daha büyük bir siber saldırının öncüsü olarak da kullanılabilmektedir [21-22-23]. Bu tip saldırılar, kimi zaman Balküpü (İng.Honeypot) sunucuları kullanılarak erken tespit edilebilmektedir [24]. Balküpü tekniği kullanılarak web saldırılarının genel olarak nasıl gerçekleştirildiği ve yayıldığı konusunda Canali ve Balzarotti [25], bir dizi farklı hizmeti barındıran, tamamen işlevsel 500 bal küpü web sitesinden oluşan bir ağın tasarımını, uygulamasını ve dağıtımını 100 günlük deneylerde yaklaşık 6.000 saldırı sırasında oluşturulan 85.000'den fazla dosya üzerinden incelemişlerdir.

Bir DDoS saldırısında bir web sitesi birden fazla kaynaktan gelen trafikle bombardımana tutulur, sunucuya tahribat verilerek çökmesine neden olunmaktadır. Bu saldırıların siyasi ve dini nitelikli olduğu bazı olaylar da sıklıkla görülebilmektedir. Örneğin geçtiğimiz yıllarda Türk bilgisayar korsanları, Danimarka'da yayınlanan bir gazetede yer alan ve Hazreti Muhammed'in ortasında bomba olan bir türbanla çizildiği bir karikatürü yayınlayan veya tartışan Avrupa'nın binlerce web sitesini tahrif edilmiştir [26]. Yakın dönemde yaşanan Rusya ve Ukrayna arasındaki savaşın siber dünyadaki boyutunu inceleyen Vu vd., [27] 358 bin web tahrifat saldırısı ile 1,7 milyon zombi bilgisayarın katıldığı DDoS saldırısı ve işgalden iki ay önce ve dört ay sonra gönüllü bir hack tartışma grubunun 441 duyurusunu incelemiştir. Söz konusu çatışmanın düşük seviyeli siber suç topluluğunun dikkatini kısa süreli ama önemli ölçüde çektiğini, Rusya ve Ukrayna'yı hedef alan hem tahrifat hem de DDoS saldırılarında kayda değer artışlar olduğunu ortaya çıkarmışlardır.

Bu noktada kuşkusuz mahremiyet, yanlış pozitif denetimi ve yasal süreçlerin işletilmesi konusunda çeşitli çatışma alanlarına dikkat edilmesi de gerekmektedir. Örneğin, saldırıları izlemek ve etiketlemek için kullanılan teknikler, kullanıcıların veya müşterilerin mahremiyetini ihlal edebilir. Bu nedenle saldırı izleme ve etiketleme süreçleri sırasında gizlilik ve veri koruma önlemlerinin dikkate alınması önemlidir. İkinci olarak, saldırıları otomatik izleyen ve etiketleyen sistemler, zaman zaman yanlış pozitif sonuçlar verebilir. Bu, normal kullanıcı etkinliklerinin yanlışlıkla saldırı olarak işaretlenmesine yol açabilir ve yanlış alarmlara neden olabileceğinden dikkatle hareket edilmesi gerekmektedir. Saldırılarla ilgili tespit ve etiketleme verilerinin yasal süreçlerde delil olarak kabul edilebilmesi için uygun zincirleme kanıtların korunması önemlidir. Sonuç olarak web servis saldırılarının izlenmesi ve etiketlenmesi güvenlik açısından önemli bir adımdır ve saldırıları tespit etmeye, savunma mekanizmalarını geliştirmeye ve hızlı bir şekilde müdahale etmeye yardımcı olur. Ancak bu süreçlerin etik kurallara uygun bir şekilde uygulanması ve veri güvenliği dikkate alınarak yapılması sanal dünyada en dikkat çekici politikalar arasında gösterilmektedir.

2. ÖNCEKİ ÇALIŞMALAR

Zone-H ve web saldırı üzerine yapılan bazı araştırmalar, Zone-H sisteminin siber güvenlik alanındaki etkisini ve rolünü değerlendirmek için yapılmıştır. Siber saldırılar temelde etik ve etik olmayan ya da yasal ve yasal olmayan gibi farklı değerler üzerine inşa edilmektedir. Bu çalışmaların bazılarında geçmiş saldırı verilerinin nasıl kullanıldığı irdelenmiştir [28]. Zone-H sisteminin saldırıları tespit etme ve analiz etme yetenekleri, çeşitli araştırmalarda ayrıntılı bir şekilde incelenmiştir. Örneğin Moneva vd., [29] araştırmalarında çevresel kriminoloji perspektifinden web sitesi tahrifatlarında tekrarlanan mağduriyetin dört önermesini test etmişlerdir. İlgili veri kümesi diğer değişkenlerin yanı sıra, tahrifat yapanların bir saldırıyı kaydetmek için talepte bulundukları tarih, takma adları, motivasyonları, tahrifat için kullanılan saldırı türü, tahrif edilen web sitesinin URL'si ve saldırının daha önce kaydedilmiş bir alan adının yeniden tahrifatı olup olmadığı hakkında 1 Ocak 2010- 4 Nisan 2017 arasındaki verileri incelemişlerdir.

Van de Weijer vd., [30], benzer bir şekilde araştırmalarında Zone-H vakalarını web tahrifatları gerçekleştiren aktif bilgisayar korsanlarının gelişimsel yörüngeleri üzerinden ele almışlardır. Bu kapsamda Ocak 2010 ve Mart 2017 tarihleri arasında saldırı incelendiğinde; web sitelerine yönelik tahrifatların çoğunu küçük bir tahrifatçı popülasyonu oluşturduğunu ve geleneksel suç türleriyle bazı ortak ilişkiler olduğunu ortaya çıkarmışlar ve siber saldırı yapanların yöntemleri ve hedefleme uygulamaları itibariyle genel olarak tahrifatları gerçekleştirme sıklıklarına göre farklılık gösterdiğini bulgulamışlardır.

Bazı alışmalar, Zone-H verilerini makine öğrenmesi yöntemiyle analiz ederek siber saldırı trendlerini belirlemeyi amaçlamıştır. Davanzo vd, makine öğrenimi tekniklerine dayalı olarak izlenen sayfanın profilini otomatik olarak oluşturarak sistem performansını 3 ay boyunca gözlemlemişlerdir. Araştırmada 320 gerçek tahrifat içeren 300 yüksek dinamik web sayfasından oluşan bir veri kümesi üzerinde yanlış pozitifler ve yanlış negatifler açısından değerlendirilmiştir [31], Siber dünyada yapılan saldırıların önemli bir gerekçesi "kültürel psikoloji" olarak kabul edilmekle birlikte, "kültürel farklılıklar" [33-34-35], konusu da siber saldırıların bir sebebi olarak görülebilmektedir. Bu bağlamda üretilen bir dizi çalışma içerisinden Zone-H verilerini kullanarak güvenlik uzmanlarına saldırı eğilimleri ve savunma stratejilerini kültürel farklılıklar ve kültür boyutları üzerinden inceleyen çalışmalar da yer almaktadır.

Sample vd., [36], 2005'ten 2014'e kadar 36 ülkede kendini tanımlayan saldırganlar için toplanan Zone-H verileri 7 farklı saldırı vektörü boyunca incelenmiştir. Bu veriler bağlamsal amaçlarla Hofstede'nin kültürel çerçevesi kullanılarak incelenmiştir. Bulgular benzersiz kültürel özelliklerle ilişkili birkaç saldırı vektörünü gösterirken, diğer saldırı vektörlerinin sonuçları daha genel özelliklerle sınırlı kaldığını ortaya çıkarmıştır. Zone-H sistemi üzerine yapılan araştırmalar içerisinde hacker davranışlarını genellikle veri analitiği, saldırı sınıflandırması ve güvenlik stratejileri gibi konular bağlamında ele alan çalışmalar da bulunmaktadır.

Siber suç kriminolojisi üzerine Ooi vd., [37] teorik model tabanlı araştırmalarında yalnızca son beş yıl içinde katılan 1,946 saldırganlari baz almışlardır. Zone-H sisteminden toplanan orijinal veriler, 29 Şubat 2000 ile 9 Nisan 2010 tarihleri arasında toplanan 30.627 bilgisayar korsanlığı biriminin 3.545.153 gözlemini içermektedir. En son hacker davranışlarının verilerini yakalamak için bilgisayar korsanları çeşitlilik arama davranışlarını açıklayan teorik bir model geliştirmekte ve bu modelin ön testini yapmaktadır. Zone-H sisteminin kimi zaman politik tabanlı gerekçelerle ile siber saldırılara dönüşebilmesi de mümkün olabilmektedir. Türkiye ve Hollanda arasında son yıllarda yaşanan "Karikatür krizi" sonrası "2017 seçim referandumu sürecinde" yaşanan diplomatik kriz, siber-savaş olarak dönüşmüştür. Romagna ve Van Den Hout [38], tarafından Ocak 2016-Aralık 2016 dönemi için Zone-H arşivindeki saldırı verilerine bakılarak nicel analiz gerçekleştirilmiştir. Bu analiz süreci ilgili kriz ile siber ortamdaki saldırıların ilişkisine odaklanmıştır.

WEB SERVİSLERİNİN İZLEME POLİTİKALARI

Web servislerinin izlenmesi, servislerin kullanıcı deneyimlerinin özelliklerine bağlı olarak denetiminden performans süreçlerine kadar geniş bir izleme alanını temsil etmektedir. Bu konuda özellikle web servislerinin performansının izlenmesi taleplere yanıt verme süresi, işlem başına harcanan zaman ve genel hız açısından gerçekleştirilmektedir. Bu şekilde performans düşüklükleri veya kaynak kullanımındaki anormallikler belirlenebilmekte ve gerekli önlemler alınabilmektedir. İkinci aşamada web servislerinde meydana gelen hatalar ve sorunlar izlenerek erken müdahale ile sistem kesintileri veya hataların etkileri minimize edilebilmektedir. Aynı zamanda kullanıcıların yaşadığı sorunların hızlıca tespit edilip çözülmesi sağlanabilmektedir. Kullanılabilirlik kontrolü, web servislerinin kullanılabilirliği izlenerek kullanıcıların erişimine ve hizmetlere engel teşkil eden potansiyel sorunlar tespit edilir ve çözülmesinde önemli bir denetleme mekanizması olarak kabul edilmektedir.

Web servislerinin genel kaynak kullanımının takibi (örn. CPU, bellek, ağ bant genişliği) gibi ortamların izlenerek gereksiz yüklenmelerin engellenmesine veya kaynak tükenmelerinin önlenmesine katkı sağlamaktadır. Bu, verimli ve etkin bir sistem yönetiminin önemli bir koşulunu oluşturmaktadır. Güvenlik izlemesi ise web servislerinin güvenlik durumu izlenerek potansiyel güvenlik açıkları veya saldırı girişimleri tespit edilir ve siber güvenlik önlemleri alınması konusunda yönlendirici bir rol oynayabilmektedir. Web servislerinin izlenmesi için genellikle özel izleme araçları ve yazılımları kullanılır. Bu araçlar sistem yöneticilerine, geliştiricilere ve ağ yöneticilerine gerçek zamanlı olarak güncel bilgiler sunar ve kritik öneme sahip verilerin korunmasını sağlayabildiğinden izleme verilerinin takibi ile gelecekteki kapasite planlaması ve sistem iyileştirmeleri için de etkileşim ortamı oluşturabilmektedir.

2.1. Web Servislerinin Saldırı Tipolojileri

Web saldırıları farklı amaçlarla gerçekleştirilebilmektedir. Bu saldırılar konusunda ilk akla gelen sosyo-psikolojik gerekçeler saldırganların kişisel ve toplumsal motivasyonlarından kaynaklanmaktadır. Bu motivasyonlar saldırganların davranışlarını etkileyen sosyal ve psikolojik faktörlerden beslenebilmektedir. Saldırganların farklı ruhsal motivasyonlara ve politik süreçler ile ekonomik davranış setlerine sahip olmaları da bu süreçleri şekillendirebilmektedir.

Mondragón vd., devlet kurumlarının web sitelerine odaklanmış olan bu saldırı türünün kontrol altına alınması ve raporlanması için bir güvenlik kontrolünün oluşturulmasına yönelik bir model geliştirilmesini önerdikleri çalışmada, kaynak kodun belirli bölümlerinin sürekli okunması yoluyla web sitelerine yapılan saldırıların çevrimiçi olarak kontrol edilmesi dışında, bilginin bütünlüğünün tespit edilmesini ve korunmasını sağlamak üzere şekillendirilmişlerdir [39]. İnternet güvenlik tehditleri genellikle bir web sitesinin hileli bir şekilde değiştirilmesini, genellikle de hiçbir sayfanın bulunmaması gereken URL'lere yeni sayfalar eklenmesini içermektedir. Web servis saldırıları, web servislerine yönelik yapılan kötü niyetli girişimlerdir. Bu saldırılar web servislerinin güvenlik açıklarından yararlanarak hizmetleri bozma, veri hırsızlığı veya yetkisiz erişim gibi zararlı faaliyetleri içerebilmektedir.

Web servis saldırılarının sosyo-psikolojik gerekçelerinden güç ve kontrol ihtiyacı, bazı saldırganların web servislerine saldırarak güç ve kontrol hissi elde etmeye çalışmasını ifade etmektedir. Bu tür saldırganlar siber alanda yeteneklerini göstermek ve kendilerini üstün hissetmek için saldırıları kullanmaktadır. Bazı saldırganlar siber alanda statü ve saygınlık kazanmak amacıyla saldırılar gerçekleştirir. Başarılı bir saldırının bu kişilere siber topluluk içinde itibar kazandırabileceği eylemlerin ard alanını oluşturmaktadır. Web servis saldırılarının arkasında bazen kişisel veya toplumsal öfke ve intikam arayışının yatması bir başka sosyo-psikolojik faktör olarak dikkat çekmektedir. Saldırganlar, hedef gördükleri kurum veya kişilere zarar vermek için siber saldırıları bir araç olarak kullanabilmektedir. Grup baskısı ve toplumsal etkileşim, saldırganların siber gruplar veya hacker

toplulukları içinde yer alarak grup baskısı altında saldırıları gerçekleştirebilmesine neden olabilmektedir. Zira toplumsal etkileşim ve grup normları saldırganların davranışlarını tetiklemektedir.

Bu saldırıların dışında önemli iki faktör olarak "ekonomik" ve "politik" gerekçeler de bulunmaktadır. Saldırganlar web servis saldırılarını maddi kazanç veya finansal amaçlar için gerçekleştirebilirler. Örneğin, veri hırsızlığı, fidye saldırıları veya kredi kartı bilgilerini ele geçirme amacıyla yapılan saldırılar bu kategoriye girmektedir. İdeolojik ve siyasi nedenler bazı saldırganların web servislerine saldırı yapabilmesinde etkin olabilmektedir. Saldırılar belirli bir politik veya ideolojik mesajı yaymak veya karşıt bir ideolojiyi bastırmak amacıyla gerçekleştirilebilir. Son yıllarda dini ve milli konularda yaşanan politize edilen fikirlerin "intikam" olarak düşünülmesi, sanal mecralarda siber saldırı şeklinde dönüşmesine zemin hazırlayabilmektedir.

Bazı saldırganlar, teknik becerilerini test etmek veya siber dünyayı keşfetmek amacıyla da web servislerine saldırı yapabilmektedir. Bu tür saldırılar, genellikle zarar verme amacı taşımaz, ancak hedef sistemlere rahatsızlık verebilmektedir. Ancak veri Botnet oluşturma gibi eylemlerde saldırganlar web servislerine saldırarak etkilenen cihazları bir Botnet ağına dönüştürebilmektedir. Bu Botnet ağları, saldırganların daha büyük hedeflere saldırmak veya spam, e-posta göndermek gibi amaçlarla kullanılabilmektedir. Saldırganlar, veri hırsızlığı amacıyla web servislerine saldırarak kullanıcıların kişisel bilgilerini, finansal verilerini, gizli şirket bilgilerini veya diğer hassas verileri çalmayı hedefleyebilir. Bu bilgiler daha sonra kötü niyetli faaliyetlerde kullanılabilir, satılabilir veya şantaj amacıyla kullanılabilmektedir. Saldırganlar bir web servisinin hizmetini engellemek için saldırı gerçekleştirebilmektedir.

Bu tür web saldırıları sunuculara yoğun talepler göndererek kaynakların tüketilmesine neden olabilmekte veya hizmetin normal işleyişini bozabilmektedir. Bu durum, web servisini kullanılamaz hale getireceğinden ciddi maddi zararlara neden olabilmektedir. Bu noktada saldıran kişinin eylemini kendi adına mı yoksa rakip bir şirket ya da devlet adına yapıp yapmaması belirleyici olabilmektedir. Bir rakip şirket ya da devletin yurttaş verilerine erişerek stratejik bilgilerini ele geçirmek ve bu bilgileri rekabet avantajı sağlamak için kullanmak sıklıkla görülen bilişim suçları arasında yer almaktadır.

Web servis saldırıları konusunda SQL enjeksiyonu, XSS, CSRF, XML, RFI, LFI gibi çeşitli yöntemler bulunmaktadır. SQL enjeksiyonu, saldırganın web servislerine gönderilen verileri kötü niyetli SQL kodlarıyla manipüle ederek veritabanı üzerinde yetkisiz işlemler gerçekleştirmeye çalışması olarak tanımlanmaktadır [41]. XSS (Cross-Site Scripting) saldırısı, saldırganın web servisi kullanıcılarının tarayıcılarında çalışacak kötü niyetli betikler enjekte ederek kullanıcıları hedef almasıdır. Bu saldırganlar, kullanıcıların oturum bilgilerini çalabilmekte veya istismar edebilmektedir [42-43-44]. CSRF (Cross-Site Request Forgery) saldırısında kullanıcıları güvendiği bir web sitesine yönlendirir ve bu site üzerinden yetkisiz istekler hacker tarafından gönderilmektedir. Bu saldırı, kullanıcının tarayıcısı üzerinden gerçekleştiği için kullanıcının yetkisi olmadığı bir işlemi gerçekleştirebilmesi şeklinde açıklanabilmektedir [45].

XML Kök Saldırısı (XML Entity Expansion); saldırgan XML işleme motorlarını aşırı yüklemek amacıyla çok sayıda varlık bildirimi göndererek hizmetin aşırı yüklenmesine neden olabilmektedir [46]. Servis Reddi Saldırıları (Denial of Service-DoS); saldırgan, web servisine yoğun talepler göndererek kaynakları aşırı yükleyebilmekte ve hizmetin çökmesine veya erişilemez hale gelmesine neden olabilmektedir [47-48-49-50]. XML Yakınsama Saldırısı (XML Schema Poisoning); saldırgan, kötü niyetli XML şemaları kullanarak web servisi tarafından yapılan veri doğrulamalarını aşabilir veya bozabilmektedir [51]. Bu tip saldırılar, veri bütünlüğünü ve güvenliğini riske atabilmektedir [52]. Web servis saldırılarının izlenmesi ve etiketlenmesi için saldırı izleme altyapısı kurarak web servislerinin trafiğini izleyebileceğiniz bir izleme altyapısı oluşturulması adına saldırı tespit sistemi/saldırı önleme sistemi (WAF, IDS ve IPS) veya güvenlik olay yönetimi sistemleri gibi teknolojiler kullanmak önemlidir [53].

Web servis trafiğini kaydeden ve analiz eden bir veritabanı veya günlük dosyası oluşturarak izleme altyapısı aracılığıyla web servis trafiğinin kaydedilmesi gerekmektedir. İlgili verilerin analiz edilerek saldırı türlerini, hedefleri, kaynakları ve diğer önemli bilgileri belirlemek için veri madenciliği veya analitik araçlar kullanılması tercih edilmelidir [54]. Web servislerinin saldırılarında analiz sonuçlarına dayanarak saldırıların sınıflandırılması ve etiketlenmesi, saldırıların tipolojilerinin belirlenmesi (örneğin, SQL enjeksiyonu, kimlik avı, DDoS saldırısı vb.) için etkili bir yöntemdir [55]. Bu çözümlere ek olarak saldırıların karmaşıklık düzeylerine ve zarar potansiyellerine göre etiketler atamak (örneğin; düşük, orta veya yüksek risk), toplanan veriler üzerinde trend analizi yaparak saldırı trendlerini belirlemek, elde edilen verileri, saldırı trendlerini ve önlemleri diğer siber güvenlik uzmanları ve kuruluşlarla paylaşıp iyileştirmek önemli stratejiler şeklinde değerlendirilmektedir. Sistem üzerinde sürekli olarak izleme sürecini iyileştirmek, yeni saldırı türlerini tanımlayabilmek ve önlemleri güncellemek gerekmektedir. Zira bu yöntemler, web servis saldırılarının izlenmesi ve etiketlenmesi için genel bir rehber niteliğindedir. Her organizasyonun ve siber güvenlik ekibinin ihtiyaçlarına ve kaynaklarına göre bu süreci özelleştirebilmek ve geliştirebilmek için etkin politikalar gereklidir.

3. HACKER ETİKETLEMELERİ

Web servis saldırıları sürekli olarak evrim geçirir. Bu nedenle web servis sağlayıcılarının güvenlik önlemlerini güncel tutması ve düzenli olarak saldırı tespit ve önleme mekanizmalarını kullanması önemlidir. Bilgisayar ve benzer araçlarla internet üzerinden yapılan saldırılar siber saldırı, tahrifat ve hackleme gibi farklı isimlerle tanımlanmaktadır. Hack bir tür kriminolojik durum ve suç konusunu oluşturmakla birlikte bazı görüşlere göre "anti-bürokratik yapıya karşı kahramanlık" [56] olarak tanımlanmakta, "programların özgürleşmesi ve zihin ile ruhun estetik biçimleri" [57] şeklinde de kabul edilebilmektedir.

Siberuzamda yapılan her türlü zararlı eylemi yapan kişi, grup ya da topluluk tarafından sanal dünyada izi bırakılmaktadır. Bu iz bırakma ve eylem etiketlenmesi, bilgisayar korsanlarının saldırı yaptıkları ve ele geçirdikleri sitelerde kimi zaman kendi imzaları, logoları ve isimleri üzerinden geniş kitlelere duyurulması biçiminde gerçekleşmektedir. Bu konu internet üzerinden zararlı işlemler gibi görülmekle birlikte sistemlere verilen zararların fidye ün kazanma ve keyif için yapılması, suç eyleminin "yumuşak hırsızlık" [58], "dijital etik ikilemi" [59] ve hack konusunda "etik belirsizlikler" [60] şeklinde anlamsız hale geldiğini göstermektedir. Bu konuda Moores ve Chang, [61] gerçek dünya ile sanal dünyadaki etik ikilemlerin suç konusuna ve eylemlere etki edebildiğine değinmektedir. Bu noktada suç ve suça karşı bakış açısındaki çatışma, saldırı ve hack eylemlerinde eylemi yapan kişi ya da kişilerin kendilerini suç kaynağıyla "etiketleme" gibi karmaşık bir davranışın ortaya çıkmasına da neden olabilmektedir.

Sanal dünyada yapılan bu etiketleme hali, "hacker taggers" [62-63] şeklinde tanımlanmaktadır. Bu eylem kimi zaman kanıt konusu olan eylemin sahte olması veya üçüncü kişilerce de onaylanması adına alternatif mecralara da ihtiyaç duyulmasına neden olmaktadır. "Hacker Taggers" [64-65] terimi, hacker veya siber güvenlik uzmanlarının web sitelerini, uygulamaları veya sistemleri hacklemiş oldukları durumları, genellikle sanal bir işaret veya imza bırakarak belirtmeleri anlamına gelir. Bu işaretler veya imzalar genellikle bir kod parçası, mesaj, resim veya dosya şeklinde olabilir ve saldırganın yapılan eylemi, yeteneklerini veya kimliğini göstermek hatta geniş kitlelere mesaj iletmek amacı taşıyabilmektedir.

Saldırı etiketlemesi, eyleminin temelinde saldırıları duyurmak, başarılarını göstermek, gurur duydukları bir eylemi işaretlemek veya diğer hacker kişilerle etkileşimde bulunmak gibi çeşitli nedenlerle de bırakılabilmektedir. Bu etiketler, bilgi güvenliği uzmanları tarafından saldırıların izini sürmek ve saldırganların motive edici veya mesajlarını anlamak için incelenebilmektedir. Hatta bir noktada etik olmayan ve yasa dışı saldırılar anlamına gelebilir. Yetkisiz erişim ve veri hırsızlığı gibi eylemler, yasalara aykırıdır ve ciddi sonuçlar doğurabilir. Etik hacker olarak tanımlanan kişi ya da

gruplar, siber güvenlik uzmanları ve etik güvenlik testi yapan kişiler, yalnızca yasal izinlerle ve sorumlulukla gerçekleştirdikleri güvenlik testlerinde herhangi bir iz bırakmamak için özen gösterirler. Onların amacı sistem sahiplerine zayıf noktaları bildirmek ve güvenliği artırmaya yardımcı olmaktır.

Siber güvenlik saldırganlarin ve kötü niyetli saldırganların neden olduğu tehditlere karşı bilgisayar sistemlerini, ağları ve dijital verileri koruma sürecini ifade eder. Bu bağlamda web servisleri siber güvenlik açısından potansiyel hedeflerdir. Saldırganlar web servislerine yönelik saldırılarla veri ihlalleri, kimlik hırsızlığı, veri manipülasyonu ve hizmet kesintileri gibi tehditler yaratabilmektedir. Bilgisayar sistemlerine ve ağlara izinsiz olarak giren ve bu sistemleri kötü amaçlar için kullanan kişiler beyaz şapkalı, gri şapkalı ve siyah şapkalı olarak farklı kategorilere ayrılırlar. Beyaz şapkalı hackerlar, siber güvenlik uzmanları ve etik hackerlardır; sistemleri güvende tutmak ve güvenlik açıklarını tespit etmek için çalışırlar.

Etik saldırganlar (hacker) genellikle beyaz şapka saldırganlar ile eş anlamlı olarak kullanılır. Bu terim, bilgisayar sistemlerini test ederek güvenlik açıklarını bulan ve düzeltmeye yardımcı olan kişileri tanımlamaktadır [66]. Etik saldırganlar, ağ güvenliğini ve siber güvenlik önlemlerini geliştirmeye odaklanırlar. Gri şapkalı saldırganlar hem iyi niyetli hem de kötü niyetli faaliyetlerde bulunabilirler ve etik olmayan yöntemlerle bilgisayar sistemlerine erişebilirler. Siyah şapkalı saldırganlar ise kötü amaçlı faaliyetlerde bulunan ve zarar veren kişilerdir. Siyah şapka saldırganlar web sistemlerine zarar vermek, hırsızlık yapmak veya diğer kötü niyetli faaliyetlerde bulunmak amacıyla hareket etmektedir.

3.1. Zone-H ve Siyah Şapkalı Hacker Etkileşimi

Zone-H, tahrif edilmiş web sitelerini tahrif edenlerin kendi raporlarına dayanarak arşivleyen özel bir web sitesidir. Tipik olarak bir bilgisayar korsanı bir web sitesini tahrif ettiğinde tahrif olayının ayrıntılarını Zone-H web sayfası aracılığıyla Zone-H'ye bildirir. Bildirilen bilgiler arasında tahrif edilen web sitesinin URL'si, tahrifatın nedeni (örn. eğlence için, siyasi nedenlerle, en iyi tahrifatçı olmak için, vb.), hackleme yöntemi (örn. SQL enjeksiyonu, bilinen güvenlik açığı, vb.), kurbanın işletim sistemlerinin türü (örn. Linux, Solaris, Win XP, MacOS, vb.) ve bildirimde bulunan kişinin kimliği yer alır. İhlallerin nedenleri saldırı şekli ve işletim sistemi türleri Zone-h.org tarafından önceden tanımlanmış olan açılır listelerden ihbarda bulunan hacker birimi tarafından seçilir. Zone-H'nin web sunucusu ihbar anında tahrif edilmiş web sayfasını otomatik olarak yakalar. Yakalanan web sayfası sahte raporları elemek için Zone H personeli tarafından manuel olarak doğrulanmaktadır.

Zone-H gibi etiket eylemini yapan gruplar, bunu mirror (el geçirilen sayfanın ekran görüntüsünün kaydı) olarak dijital mecralara kaydetmektedir. Bu "etiket" saldırı yapan kişi ve grupların "Notifier" şeklinde puanlanarak güncellenmesidir. Bilgisayar korsanları bu konuya kimi zaman bilgisayar korsanlığına ait bir yarışma olarak odaklanmakta, veri çalmayı ya da çevrimiçi hizmetlerin işleyişini bozmayı amaçlamamakta, sadece arkalarında bir "etiket" bırakmayı hedeflemektedirler [67]. Woo, Kim ve Dominick [66] tarafından yürütülen bir çalışmada tahrif edilmiş 462 web sitesi analiz edilmiştir. Araştırma bilgisayar korsanlarının tahrifat yapmak için farklı motivasyonlara sahip olabileceğini, en yaygın olanlarının psikolojik ve siyasi olduğunu doğrulamıştır. Woo vd., bilgisayar korsanlarının genellikle arkalarında hack taggers olarak "sataşmalar, selamlar ya da kartvizitler" bıraktıklarını belirtmektedir [66].

Zone-H sistemi ve siyah şapkalı hackerlar arasındaki ilişki karmaşık ve çeşitlidir. Zone-H sistemi, gerçek zamanlı olarak siber saldırıları izleyen ve kaydeden bir platform olarak bilinirken siyah şapkalı saldırganlar ise siber güvenliği ihlal etmek amacıyla bilgisayar sistemlerine yetkisiz olarak giren ve zararlı faaliyetlerde bulunan kişileri ifade etmektedir.

Zone-H modeli, siber saldırıları izleme ve kaydetme yetenekleriyle siber güvenlik uzmanlarına ve araştırmacılara değerli bir kaynak sağlar. Bu veritabanı dünya genelinde gerçekleşen saldırıları toplayarak saldırı trendlerini analiz etmeyi ve saldırganların motivasyonlarını anlamayı mümkün kılar.

Zone-H, saldırıları sınıflandırma, saldırı tiplerini belirleme ve savunma stratejilerini geliştirme gibi konularda önemli bir bilgi kaynağı olarak hizmet eder. Siyah şapkalı saldırganlar, Zone-H sisteminin izlediği ve kaydettiği saldırıları gerçekleştiren kişiler olabilir. Zone-H veritabanında kaydedilen saldırılar genellikle zararlı ve yetkisiz faaliyetleri içerir. Siyah şapkalı hackerlar, bilgisayar sistemlerine yetkisiz erişim sağlayarak kişisel bilgileri çalmak, ağları felç etmek, fidye yazılımları yaymak veya başka zararlı faaliyetlerde bulunmak gibi niyetlerle hareket etmektedir.

Bununla birlikte, Zone-H sistemi siyah şapkalı hackerları sadece izlemekle kalmaz, aynı zamanda bu tür saldırıları önlemek için de bir kaynak olabilir. Zone-H'nin sağladığı saldırı verileri, siber güvenlik uzmanlarına ve savunma ekiplerine, siyah şapkalı hackerların kullanabileceği güvenlik açıklarını belirleme ve saldırıları engelleme konusunda önemli bilgiler sunabilir. Bu sayede Zone-H sistemi, siyah şapkalı saldırganlar ile mücadelede etkili bir rol oynayabilmek ve siber güvenliği güçlendirmeye yardımcı olabilmek adına değerlendirilebilmektedir.

3.2. Siber Suç ve Uluslararası Düzenlemeler

Web sayfasına saldırı, bir kişi veya kuruluşun izinsiz olarak bir web sitesine erişim sağlama, veri çalma, zarar verme veya başka herhangi bir şekilde yetkisiz giriş yapma eylemidir. Bu tür saldırılar, dijital ortamda ciddi sonuçlara yol açabilir ve hukuki sonuçları da vardır. Web sayfasına saldırı, uluslararası hukuk açısından siber suçlar kategorisine girmektedir. Bilgisayar Suçlarına Karşı Avrupa Siber Suç Sözleşmesi 2001 yılında imzalanmış ve 2004 yılında yürürlüğe girmiştir [68]. Uluslararası Telekomünikasyon Birliği (ITU) Siber Suçlarla Mücadele Tüzüğü ve 1961 Budapeşte Sözleşmesi (Extradition Convention) olarak diğer düzenlemeler de yer almaktadır. Budapeşte Sözleşmesi [69], bazı suçların ortak tanımını yapmak suretiyle, ulusal düzeyde mevzuatın uyumlulaştırılmasını mümkün kılmak; siber suçların soruşturulması açısından bilişim ortamına uygun düşen ortak yetkileri tanımlayarak, devletler arasındaki muhakeme kurallarının oluşturulmasını sağlamak hem geleneksel hem de yeni türden uluslararası iş birliği yöntemlerini belirleyerek, devletlerin bu hükümleri bir an önce uygulamasını aktif hale getirmek [70] üzere düzenlenmiştir.

Kerr'e göre Siber suç mevzuatı yeni oluşmakta olan bir mevzuattır ve bu nedenle değiştirilmeye son derece açıktır [71]. Bu noktada özellikle Moitra, "Yeni bir suçluluk türü söz konusu olduğundan, ceza adaleti sisteminin birçok aktörünün konuya henüz alışkın olmadığını" [72] belirtmektedir. Bununla birlikte siber suçun önlenmesi, yeni düzenlemelerin birlik içinde ve birlik dışındaki alanlarda da etkin biçimde uygulanması adına stratejik eylemler yapılmaktadır. [69-73]. 1980 sonra liberalleşen dünyada hukuki süreçlerin de yenilenmesi ihtiyacı karşısında öncelikle küresel düzeyde iş birliği, farkındalık ve etkin mücadele politikaları da oluşturulmaya başlanmıştır [74].

İnternet alanındaki gelişmelerin tek yönlü iletişim akışından çoklu ve etkileşimsel süreçlere dönüşmesi dışında verilerin ele geçirilmesiyle yapılan şantajlar ve mahremiyet sorunsalı karşısında yasal düzenlemeler aynı hızda gerçekleştirilememektedir. Avrupa Konseyi Sanal ortamda İşlenen Suçlar sözleşmesi [75], olarak bilinen Siber Suçlar Sözleşmesi dört kategoride dokuz suçun cezalandırılmasını öngörmektedir. Sözleşme, internet ve diğer bilgisayar ağları üzerinden işlenen suçlara ilişkin ilk uluslararası anlaşma olup, özellikle telif hakkı ihlalleri, bilgisayarla ilgili dolandırıcılık, çocuk pornografisi ve ağ güvenliği ihlallerini ele almaktadır. Ayrıca, bilgisayar ağlarının aranması ve dinleme gibi bir dizi yetki ve usulü de belirtmektedir. İlk kategori "sulha karşı suçları", ikinci kategori, "bilgisayarla ilgili suçları", cezai yaptırım gerektiren hükümler hedeflemektedir. Üçüncü kategoriler" ırkçı ve ayrımcılık hükümlerini" dördüncü kategori ise "Telif hakkı ihlalleri ve ilgili suçları" içermektedir.

Siber suçlar konusunda ITU tarafından temelde "ITU-T X.1205 sayılı tavsiye kararında tanımlanan siber güvenliğin temel hedefleri, bilginin; "Erişilebilirlik, Bütünlük ve Gizlilik" [76] unsurlarını güvence altına almaktır. ABD küresel düzeyde bilişim suçlarının önlenmesi konusunda hızlı

düzenleme yapabilme ve diğer ülkelere bu noktada hukuki rehberlik yapabilme özellikleriyle dikkat çekmektedir. Siber suçların tespiti, önlenmesi ve müeyyidelerin uygulanması konusunda çeşitli düzenlemelere gidilmiştir. Bu noktada, USC [77], başlığı altında 1029,1030, 1362, 2511, 2701, 2702 ve 2703 yasa numaraları şeklinde düzenlenmesi yapılmıştır. Türkiye, bilişim suçlarının önlenmesi noktasında ilk düzenleme, 765 sayılı TCK'da yapılmıştır. Türk Ceza Kanunu'nda bilişim suçlarını düzenleyen 243, 244, 245 ve 246. maddeler kapsamında değerlendirilmektedir [78-79]. Özel hayat konusunda ise 135, 136 ve 138. Maddelerde bu düzenlemelere yer verildiği de görülmektedir [80]. Bunun dışında 525a, 532b, 525c, 525d, 525a ile 525c maddelerinden fail ve mağdur ile ayrıca "Fikir ve Sanat Eseri Kanunu, Tüketicinin Korunması Hakkında Kanun, Elektronik İmza Kanunu ve 5237 Sayılı Türk Ceza Kanunu" da yer almaktadır. 525a maddesi, son yıllarda bilgisayarlara yapılan saldırılarda, hackleme, veri çalma ve KVKK ile bilgi güvenliği alanlarında en çok konuşulan maddedir. 5651 sayılı kanun [81] ile internet üzerindeki suçlara ilişkin ilgili düzenlemeler ve müeyyidelerin de sınırları çizilmektedir.

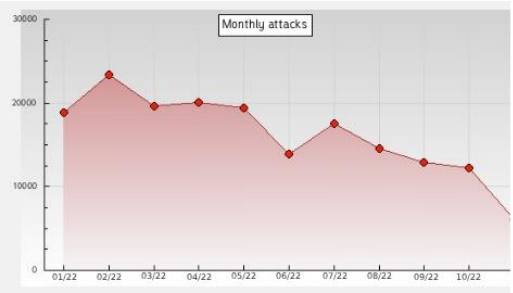
4. YÖNTEM

Zone-H, siber güvenlik uzmanlarının saldırıları izlemek ve analiz etmek için başvurdukları siber saldırılarla ilgili kapsamlı istatistikler sunan bir platformdur. Zone-H, internet üzerinde saldırıları tespit etmek için bir dizi otomatik araç kullanmaktadır. Bu araçlar, web sitelerini tarayarak saldırı girişimlerini algılamakta ve kaydetmektedir. Zone-H sisteminin altyapısı çeşitli veri tabanlarını ve kaynaklarını kullanarak saldırıları izleyip analiz etmektedir. Saldırılar çeşitli kategorilere ayrılır ve istatistiksel veriler oluşturulur. Zone-H sisteminin ana amacı saldırıları tespit etmek, saldırı yöntemlerini anlamak ve siber güvenlik uzmanlarının saldırılara karşı savunma mekanizmalarını geliştirmelerine yardımcı olmaktır. Zone-H ekibi, kendi tahrifatlarını bir takma ad altında kaydeden bireyler veya gruplar tarafından gerçekleştirilen tahrifat olaylarına ilişkin bilgileri toplamakta, doğrulamakta, depolamakta ve muhafaza etmektedir.

Bu çalışma, siber güvenlik alanında önemli bir saldırı alanını oluşturan web tabanlı saldırıların genel niteliklerini, saldırganların eylem tipolojilerini ve saldırılan sistemlerin genel nitelikleri ile bölgesel niteliklerini analiz etmek için Zone-H uygulama modeli üzerinden inşa edilmektedir. Araştırmanın temel amacı bu saldırıları, teknik ve eylem bazında sınıflandırarak etiketlenmiş saldırgan tipolojilerinin genel görünümünü ortaya çıkarmaktır. Bu kapsamda Zone-H sistemi, gerçek zamanlı tek kayıt mecrası olduğu için seçimlenmiş ve ilgili verilerin analizi için bir (1) aylık sistem incelemesi yapılmıştır. Araştırmada saldırgan (hacker) kimlikleri ile saldırılan mecraların sayısal ve teknik özellikleri 1-31 Ekim 2022 tarihleri arasındaki verileri üzerinden analiz edilmiştir.

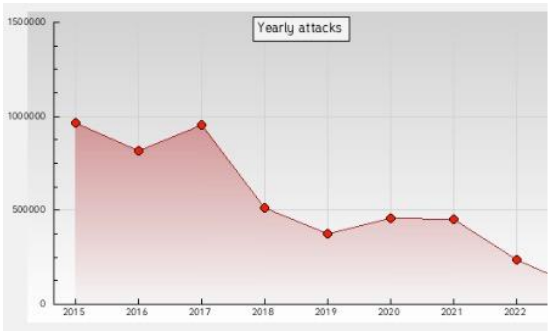
4.1. Bulgular ve Analiz

Zone-H sistemi 2002 yılında kurulan 2007 yılından itibaren hacker saldırılarının etiketlendiği bir mecra olarak internet ortamında önemli bir referans noktası olarak kabul edilmektedir. Araştırma kapsamında sitenin genel saldırı tipolojileri ve sayısal değerlerine bakıldığında http://www.zone-h.org [82] sitesi üzerinde arşiv taraması yapıldığında; güncel veriler itibariyle 105.697 tekil ip saldırısı ve 173.978 toplu tahrifat olmak üzere 279.675 toplam saldırının olduğu dijital saldırıların ise 15.210.018 düzeyinde gerçekleştiği görülmektedir. Bu sayı milyon saldırı olarak ölçümlenen sistem üzerinde genel toplamı vermemekle birlikte saldırıların an itibariyle yoğunluk düzeyleri hakkında bilgi verebilmektedir.



Şekil 1. Zone-H 01/22-10/22 Dönemi Aylık Saldırı İstatistikleri [83]

Şekil 1 ve **Şekil 2**'de yer alan aylık ve yıllık bazda saldırı istatistikleri incelendiğinde Ocak 2022 döneminden Ekim 2022 döneminde kadar olan süreçte Ocak-Şubat 2022 dönemi ile Haziran-Temmuz 2022 dönemleri dışındaki tüm aylık saldırılarda düzenli olarak düşme eğiliminin olduğu, aylık bazda 25.000 düzeyinde gerçekleşen saldırıların Temmuz 2022 dönemine kadar olan süreçte aylık bazda 7.500 saldırı seviyesine doğru evrildiği anlaşılmaktadır. Saldırıların yıllık bazda değişim oranlarına bakıldığında ise 2015 ve 2017 dönemindeki yıllık 1 milyon saldırı oranının 2016 yılında ve 2018-2022 döneminde düzenli bir biçimde düşme eğiliminde olduğu hatta yıllık bazda 125.000 saldırı düzeyine doğru değişim geçirdiği anlaşılmaktadır.



Şekil 2. Zone-H 2015-2022 Dönemi Yıllık Saldırı İstatistikleri [84]

Zone-H sisteminde "tüm zamanların en aktif bildiricileri" "ad, tekil tahribat, toplu tahribat, toplam tahribat, ana sayfa tahribatı ve yönlendirilmiş tahribat" şeklinde düzenlenmektedir. Buna göre ilk on sıra içinde "Hmei7, d3b~x, Index Php, iskorpitx, chinafans, Sejeal, 1923Turk, muhmademad, Team_CC ve imam" yer almaktadır. Bu bildiricilerin istatistiksel verileri aşağıda **Tablo 1**'de görüldüğü üzere sıralanmaktadır. Tabloda ilgili saldırı bölümleri incelendiğinde; Tekil ve yönlendirilmiş tahribatlar ile genel toplamda Hmei7 adlı kullanıcı ilk sırada yer alırken; Toplu (kitlesel), Ana sayfa ve Toplam tahribatlar (saldırılar) konusunda iskorpitx adlı kullanıcı (bildirici) ilk sırada yer almaktadır.

Tablo 1. Zone-H en yüksek 10 bildirici/hacker istatistikleri

Bildirici	Saldırı/Tahribat Tipolojileri				
	Tekli	*Toplu*	*Toplam*	*Ana Sayfa*	*Yönlendirilmiş*
Hmei7	139830	154879	294709	85387	209322
d3b~x	84239	76967	161206	21104	140102
Index Php	78964	75820	154784	9796	144988
iskorpitx	78018	393556	471574	268015	203559

chinafans	60713	53397	114110	287	113823
Sejeal	52296	53936	106232	9881	96351
1923Turk	43761	229060	272821	108401	164420
muhmademad	41141	41387	82528	10153	72375
Team_CC	38544	78463	117007	19531	97476
imam	31370	29893	61263	2268	58995

Aşağıda **Şekil 3**'te görüldüğü üzere, "Hmei7" isimli kullanıcı en yüksek bildirim sayısına sahiptir. Kullanıcının site üzerindeki temel değerleri bakıldığında 139.830 tekil IP ve 154.879 toplu tahrifat olmak üzere 294.709 toplam bildirime sahip olduğu tespit edilmiştir. Bu kullanıcının Zone-H sistemi robot uygulaması üzerinden mirror (sayfanın hack görüntüsü) ve etiketleme yapısına bakıldığında ABD merkezli bir domain (alan adı) olan Linux tabanlı ve web sunucusu bilinmeyen bir modelde ekranın erişiminin kısıtlandığı anlaşılmaktadır.

Şekil 3. Hmei7 Kodlu Hacker'e Ait Örnek Sayfa Aynalama-Etiketleme Kesiti [85]

Zone-H sistemi üzerinde 1-31 Ekim 2022 tarihleri arasında yapılan web sunucu saldırıları toplamda 968 olarak tespit edilmiştir. Bu saldırılar içerisinde en yüksek saldırı yapan 5 hacker (saldırdan) incelendiğinde; *0x1998* kodlu hacker, toplamda 250 saldırı ile ilk sırada yer alırken, genel toplam üzerinde %25,82 oranına sahiptir. *Mr.L3RBI* kodlu hacker 98 adet saldırı ve genel toplam üzerinde %10,12 oranıyla ikinci sırada yer alırken, *Temp3* kodlu hacker 74 saldırı ve %7,64 ile üçüncü sırada yer almaktadır. *Dr.3V1I* kodlu hacker 68 saldırı ve %7,02 ile dördüncü ve *Ramil Fevziyev* kodlu hacker ise 59 saldırı ve %6,09 ile beşinci sırada yer almaktadır. İlk beş sıradaki saldırganların toplamı 549 olarak saptanmış olup %56,72 toplama sahiptir. Diğer saldırganların sayısal oranı 419 ve %43,28 şeklinde gerçekleşmiştir.

Zone-H sistemi tarafından yapılan saldırı tespitlerinin sistemlerin genel görünümleri incelendiğinde ise ilgili tarihler arasındaki bir aylık izleme içerisinde 968 saldırı üzerinde 9 farklı işletim sistemi tipolojileri olduğu anlaşılmaktadır. Buna göre; *Linux* (839) adet ile ilk sırada yer alırken; *Unknown* (85 adet), *FreeBSD* (14 adet), *Win 2012* (10 adet), *Win 2008* (9 adet), *Win 2016* (5 adet), *Win 2003* (3 adet), *F5 Big-IP* (1 adet) ve *Win XP* (1 adet) olarak tespit edilmiştir. Linux tabanlı sunucu saldırıları en yoğun saldırılan sistem olarak dikkat çekerken saldırı yüzdesinin %86,67 düzeyinde genel orana sahip olduğu da görülmektedir.

Bu sistem içerisinde etiketleme alanı beş farklı şekilde gerçekleşmektedir. Bunlar Notifier olarak kullanıcı alanı şeklinde ilk etiket alanını temsil etmektedir. Bunların dışında Ana sayfa saldırısı (Homepage Defacement) H koduyla etiketlenirken, toplam 130 saldırının %13,42 düzeyinde olduğu anlaşılmıştır. Diğer etiket alanları, üçüncü düzey olarak Toplu Saldırı (Mass Defacement) M koduyla etiketlenmekte ve 688 adet saldırı %71,07 olarak saptanmıştır. Saldırı etiketleri arasında Yeniden Saldırı (Redefacement) R kodunun temel etiketi içerisinde 285 adet ve %29,44 düzeyinde olduğu anlaşılmaktadır. Son etiketleme alanı olarak IP Adres Bölgesi (IP Address Location) olarak belirlenen içerisinde ise L kodunun 62 boş olmak üzere 906 sayı ve %93,5 düzeyinde olduğu görülmektedir.

Araştırma kapsamında en yüksek saldırı düzeyime sahip olan *0x1998* kodlu hacker tarafından yapılan örnek bir saldırı aşağıda **Şekil 4**'te görüldüğü üzere "https://celebration.fl.us/phpbb/b4.html" alan adlı sitenin, Apache web sunucu üzerinde kayıtlı olduğu, ABD merkezli bir IP adresine (192.249.121.66) sahip olduğu, Linux sisteminin bulunduğu ve Hacker imzası olan görüntüde kullanıcı adının yazılı olmak üzere Mirror şeklinde etiketlendiği görülmektedir.

Şekil 4. 0x1998 Kodlu Hacker'e Ait Örnek Sayfa Aynalama-Etiketleme Kesiti [86]

Araştırma kapsamında ilgili dönem içinde saldırı yapılan ülkelerin yoğunluk değerlerine ülke bazında bakıldığında; en yüksek siber saldırıya uğrayan ülkelerin ilk üç sıralaması şu şekilde sıralanmaktadır: Endonezya toplamda 968 olarak belirlenen genel saldırı sayısı içerisinde 283 saldırı sayısı ve %29,23 ile ilk sırada yer alırken; ABD 172 saldırı adeti ve %17,76 ile ikinci ve Brezilya 66 saldırı adeti ve %6,81 genel oran ile üçüncü sırada yer almaktadır. Türkiye bu alanda 62 saldırı sayısı ve %6,40 oran ile sıralanmaktadır. Zone-H sistemi üzerinde yapılan bir aylık incelemede kamusal site olarak tanımlayabileceğimiz bel.tr ve gov.tr uzantılı sitelere yapılan saldırılara ek olarak ticari nitelikli (com ve com.tr) uzantılı siteler de dahil olmak üzere aşağıda **Tablo 2**'de yer alan veriler elde edilmiştir.

Tablo 2. Web Servis Saldırısı Yapılan Türk Siteleri

Web Servis Saldırısı Yapılan Türk Sitelerinin Tipolojileri ve Dağılımları		
Kamusal Site (bel.tr Uzantılı)		***Kamusal Site (Diğer Uzantılı Gov. vb)***
		proje.akdenizbelbir.gov.tr/kur...
		eyeterlik.cevre.gov.tr/krd.html
		yonetim.tkf.gov.tr/z.html
bogazkale.bel.tr	saphane.bel.tr	***Ticari Site (com / com.tr. vb)***
www.deredolu.bel.tr	dedeli.bel.tr/zabita.php	
kirkoy.bel.tr	corumortakoy.bel.tr/zabita.php	
solhan.bel.tr	cadirkaya.bel.tr/zabita.php	
www.degirmenayvali.bel.tr	beloren.bel.tr/zabita.php	
www.sambayat.bel.tr	ardanuc.bel.tr/zabita.php	
dagpinar.bel.tr/zabita.php	adakli.bel.tr/zabita.php	
cakirhuyuk.bel.tr/zabita.php	giresunoren.bel.tr/zabita.php	
beyhan.bel.tr/zabita.php	maden.bel.tr/zabita.php	www.ovagaz.com/z.html
balikoy.bel.tr/zabita.php	yucekapi.bel.tr/zabita.php	www.firatedas.com.tr/z.html
akharim.bel.tr/zabita.php	kocaaliler.bel.tr/zabita.php	dijitalisyerim.com/r00t.php
yayladuzu.bel.tr/zabita.php	kasrik.bel.tr/zabita.php	panel.kobiline.com/r00t.php
bereketli.bel.tr/zabita.php	karliova.bel.tr/zabita.php	raporlama.coruhedas.com.tr/z.html
tillo.bel.tr/zabita.php	ilicalar.bel.tr/zabita.php	www.ovagaz.com/z.html
konakkuran.bel.tr/zabita.php	gulsehri.bel.tr/zabita.php	www.firatedas.com.tr/z.html dijitalisyerim.com/r00t.php panel.kobiline.com/r00t.php raporlama.coruhedas.com.tr/z.html www.ovagaz.com/z.html
kizilirmak.bel.tr/zabita.php	gerger.bel.tr/zabita.php	
karssusuz.bel.tr/zabita.php	unlupinar.bel.tr/zabita.php	
karayakup.bel.tr/zabita.php	yenikentgediz.bel.tr/zabita.php	
ihlara.bel.tr/zabita.php	geyve.bel.tr	
gevas.bel.tr/zabita.php	yolalan.bel.tr/zabita.php	www.firatedas.com.tr/z.html
demirkoy.bel.tr/zabita.php	mehmetli.bel.tr/zabita.php	dijitalisyerim.com/r00t.php
taslicay.bel.tr/zabita.php	haydarli.bel.tr/dosyalar/index...	panel.kobiline.com/r00t.php
yildiz.bel.tr/zabita.php	musaltinova.bel.tr/zabita.php	raporlama.coruhedas.com.tr/z.html
harmanli.bel.tr/zabita.php	tahir.bel.tr/zabita.php	www.ovagaz.com/z.html
www.yolkonak.bel.tr	pervari.bel.tr	www.firatedas.com.tr/z.html

Bu siteler arasında bel.tr uzantılı olan siteler 50 (elli) tane olarak belirlenmiştir. Diğer kamusal nitelikli siteler 3 (üç) olup, ticari nitelikli siteler de 9 (dokuz) olmak üzere toplamda 62 (Altmış iki) sitenin bu saldırılara maruz kaldığı anlaşılmaktadır. Bu noktada saldırı yapılan sitelerin kurumsal bazda olmasına karşın tehdide açık olması ve daha çok veriye sahip olabileceği tezinden hareketle daha yoğun bir biçimde saldırıya uğrayabildiği anlaşılmaktadır.

Şekil 5. Remil Feyziyev Kodlu Hacker'e Ait Örnek Sayfa Aynalama-Etiketleme Kesiti [87]

Bu siteler içerisinde Şekil 5'te Haydarlı Belediyesi'ne ait resmi uzantılı web sayfasının "http://haydarli.bel.tr/dosyalar/index.txt" ekran görüntüsünde *Remil Feyziyev* kod adlı hacker kullanıcının mesaj ve diğer iletilerini içeren bir görsel bulunmaktadır. **Şekil 6**'da yer alan Derebolu Belediyesi'ne ait kurumsal nitelikli "http://www.deredolu.bel.tr" uzantılı web sayfasında ise *Yodo* kod adlı hacker kullanıcının mesaj ve diğer iletilerini içeren bir görsel yer almaktadır. Her iki sayfada da sunucu, IP adresleri, sistem özellikleri ile alan adları bilgileri yer almaktadır.

Şekil 6. Yodo Kodlu Hacker'e Ait Örnek Sayfa Aynalama Etiketleme Kesiti [88]

Araştırma kapsamında bulgulanan hacker tipolojileri ile etiketleme yapıları itibariyle **Şekil 3, Şekil 4, Şekil 5 ve Şekil 6**'da yer alan görseller de görüldüğü üzere farklı simge ve ikonlar ile mesajlar verdikleri anlaşılmaktadır. Her bir bildiricinin saldırı yaptığı siteye Zone-H [67] sisteminin robotu üzerinden işaretlendiği tespit edilmiştir.

5. SONUÇ

Dijital ağ politikaları ve yeni medya dijital çağda iletişim ve içerik üretiminin yönetimi ve düzenlenmesi açısından birbirini etkileyen önemli unsurlardır. Dijital ağ politikaları yeni medyanın yaygınlaşması ve gelişimi için uygun bir altyapı, düzenleme sağlayarak dijital dünyanın verimli ve güvenli bir şekilde işlemesine katkı sağlamaktadır. Aynı zamanda yeni medya içeriklerinin hızlı ve güvenilir bir şekilde kullanıcılarla buluşmasını mümkün kılabilmektedir. Dijital ağ politikaları yeni medyanın erişimini ve kullanımını düzenlemeye yönelik önemli kuralları içermektedir. İnternet hızı, veri kotaları, içerik filtrelemesi ve engellemesi gibi politikalar yeni medya platformlarının kullanılabilirliğini ve kullanıcıların çevrimiçi içeriğe erişimini sağlamak, ağların veri trafiğini yöneterek yeni medya içeriklerine kesintisiz ve kaliteli hale getirmek, veri güvenliği ve gizliliğini sağlamak için şifreleme, kimlik doğrulama ve veri koruma önlemleri gibi politikaları düzenlemek, ağların yönetimi,

izlenmesi ve performans iyileştirmeleri için gereken adımları belirlemek gibi farklı eylemleri içermektedir.

Bu çalışma Zone-H sistemi üzerinde gerçekleşen web sunucu saldırılarının analizini sunmaktadır. Elde edilen bulgular saldırıları gerçekleştiren saldırganların kimliklerini ve saldırı tiplerini ortaya koymuş, ayrıca saldırılan sistemlerin ve hedef ülkelerin dağılımını belirlemiştir. Araştırma kapsamında belirlenen Zone-H, yasadışı siber saldırıların etiketlendiği ve hacker etiketlerinin aynalama teknikleriyle kullanılabildiği tek site olduğu için tercih edilmiştir. Araştırma 1-31 Ekim 2022 tarihleri arasındaki bir aylık inceleme sürecinde gerek bildiriciler ve saldırı tipolojileri gerekse saldırıya uğrayan web servislerinin genel niteliklerini sınıflandırarak çözümlemeler getirmektedir.

Zone-H sistemi bazı verileri üyelik üzerinden kamuya sunarak istatistiksel veri erişimi için üyelik şartı getirmiştir. Analiz olarak seçimlenen tarih içerisinde elde edilen veriler, istatistiksel ve nicel değerlemeler ile incelenmiş ve yüksek kullanıcı ile düşük kullanıcı ya da saldırı düzeyleri üzerinden sıralamalar yapılmıştır. Çalışma süreci içerisinde siyah şapkalı hacker olarak tanımlanan zararlı siber saldırı yapan kullanıcıların genel özelliklerine bakıldığında 968 kayıt üzerinde özellikle çevre ülkelere ya da merkez ülkelere doğru yapılan saldırı eğilimlerinin yüksek olduğu saptanmıştır. Bu saldırı alanları içerisinde hedef noktası olarak kişisel sayfalar yerine kurumsal nitelikli sayfalara veri çeşitliliği ile kullanıcı sayılarının fazla olabileceği gerekçesiyle yönelim sağlandığı anlaşılmaktadır. Bu süreç içerisinde kullanıcı grupların eylemlerinin hukuki düzenlemelerin daha fazla ve ciddi düzeyde yaptırımlara dönüşebilmesi nedeniyle zaman içerisinde azalma olduğu ya da sisteme kayıt edilen verilerin sayısında düşme eğiliminin fazla olduğu da anlaşılmaktadır.

Bu araştırma sürecinde 1-31 Ekim 2022 döneminde 968 saldırı içerisinde 134 saldırı ülke ya da bölge bazında kategorileştirilmemiştir. Söz konusu %13,84'lük veri dışarıda bırakıldığında %86,66 oran ve 834 saldırı verisi içerisinde dağılımları itibariyle Asya kıtasının 354 saldırı ve %36,5 ile ilk sırada yer aldığı saptanmıştır. Ülke bazında Endonezya 250 saldırı ile ilk sırada yer almaktadır. Kuzey Amerika198 saldırı ve %20,45 ile ikinci sırada yer alırken, ABD 172 saldırı ile bölge ülkeleri arasında ilk sıradadır. Avrupa kıtası ise 129 toplam saldırı ve %13,32 ile üçüncü sırada bulunmaktadır. Türkiye'nin bu grup içerisinde 62 saldırı ile ilk sırada olduğu görülmektedir. Güney Amerika bölümü toplam 116 saldırı ve %11,98 ile dördüncü sırada olup Brezilya 66 saldırı ile ülke bazında ilk sırada bulunmaktadır.

Afrika kıtası 36 saldırı ve %3,71 ile dördüncü sırada yer almaktadır. Çalışmada Okyanusya Grubu'ndan Samoa ülkesi 1 saldırı ile yer alırken Ortadoğu bölümünde herhangi bir ülkeye ait veri saptanmamıştır. Araştırmada dikkat çekici bir bulgu olarak "Çin, Rusya, Japonya, Güney Kore, Hollanda ve Baltık ülkeleri gibi" yüksek internet kullanıcısına sahip olan ülkelere ait saldırı saptanmamasıdır. Bu ülkelerin dönem bazında dijital kaydının olmaması dışında siber güvenlik konusundaki yüksek ölçekli politikalarının etkinliği önemli bir değişken olarak düşünülmektedir.

Araştırmada elde edilen bulgular içerisinde belirlenen 9 farklı işletim sistemi tipolojileri olduğu anlaşılmaktadır. Bu işletim sistemleri içerisinde 839 adet ile ilk sırada yer alan Linux, siyah şapkalı hacker gruplarının dijital izlerinin takip edilmemesi için en fazla tercih ettikleri çalışma araçları olarak dikkat çekmektedir. Araştırmada Uzakdoğu ülkeleri ile Güney Amerika ülkelerinin bu alanda daha fazla etkileşim kurdukları ve merkez ülkeler olarak tanımlanan ülkelerin ağlarına sızma girişimlerinin yoğun bir düzeyde gerçekleştiği de anlaşılmaktadır.

Türkiye bu araştırma içerisinde özellikle kamu kurumlarının web servisleri ile sayfaları üzerinden saldırıya uğrayan bir ülke olarak dikkat çekmektedir. Özellikle yoğun kayıt ve kullanıcı pratiklerine hakim olan bu sitelere saldırı yapılması veri hırsızlığı konusunda bilinçli bir tercih olduğunu ve bu tür

sitelerin diğer sitelere görece daha fazla saldırıya uğrayabilmesinin siber güvenlik konusundaki yeterliliklerin de sorgulanması gerektiğini ortaya çıkarmaktadır.

Sonuç olarak Zone-H sistemi ve siyah şapkalı saldırganlar (hacker) arasındaki ilişki saldırıları izleme, analiz etme ve önleme çabalarını içeren karmaşık bir yapıda olduğu anlaşılmaktadır. Ayrıca web servislerine yapılan saldırıların giderek daha ciddi boyutlara eriştiği ve veri güvenliği konusunun da ciddi bir risk altında olduğunu ortaya çıkmaktadır. Zone-H modelinin siyah şapkalı saldırganlarin faaliyetlerini gözlemlemek ve siber güvenlik alanında koruma sağlamak için önemli bir araç olarak kullanılabilmesi, gereken önlem tipolojilerinin belirlenmesi, risklerin azaltılması ve ileriye yönelik siber güvenlik paketlerinin yeniden güncellenmesi konusunda önemli bir rol sağlamaktadır. Siber savaşların daha fazla yaşandığı yeni medya sisteminde etik ve yasal konuların da dikkate alınması gerektiği anlaşılmaktadır. Bu bağlamda Zone-H veri tabanının kullanımı ile elde edilen bilgiler ışığında güvenlik uzmanlarının saldırılara karşı daha etkili önlemler almasına ve ilgili alanlarda daha fazla araştırma yapılmasına yardımcı olacaktır.

KAYNAKLAR

[1] C. Urcuqui, M. García, J. Osorio, and A. Navarro, "Antidefacement-state of art", *Sistemas & Telemática, 14*(39), ss.9-27, 2016.

[2] Thomas J. Holt, "The Attack dynamics of political and religiously motivated hackers", in *Cyber Infrastruture Protection*, T. Saadawi and L. Jordan, Ed, Strategic Studies Institute, 2011, ss.159-180.

[3] A. W. Samuel, Hacktivism and the future of political participation, Ph.D. dissertation, in Political Science, department of Government, Harvard University, Cambridge, Massachusetts, USA, 2004.

[4] Y. Zhong, H. Asakura, H. Takakura, and Y. Oshima, "Detecting malicious inputs of web application parameters using character class sequences", In *Computer Software and Applications Conference (COMPSAC), 2015 IEEE 39th Annual*, 2(2015), Jul. 2015, ss. 525-532.

[5] X. D. Hoang, "A Website defacement detection method based on machine learning techniques". In *SoICT'18: Ninth International Symposium on Information and Communication Technology*, ACM, December 6–7, 2018, Da Nang City, Vietnam, 2018, ss.1-6.

[6] S. C. III McQuade, *Understanding and Managing Cybercrime*, Boston, USA: Allyn and Bacon, 2006.

[7] K. Cardwell, *The Best Damn Cybercrime and Digital Forensics Book Period*, New York, NY, USA: Syngres, Elsevier, 2007.

[8] M. Britz, *Computer Forensics and Cyber Crime*, 3rd ed, Upper Saddle River, Pearson, NJ, USA, 2013.

[9] B. Arief, M.A. Bin Adzmi, and T. Gross, "Understanding cybercrime from its stakeholders'perspectives: Part 1 attackers", *IEEE Security & Privacy, 13*(1), 2015, ss.71-76.

[10] M. Chawki, A. Darwish, A. Mohammed, and S. Tyagi, *Cybercrime, Digital Forensics and Jurisdiction*, New York, NY, USA: Springer International Publishing, 2015.

[11] R. Sabillon, J. Cano, V. Cavaller, and J. Serra, "Cybercrime and cybercriminals: A Comprehensive study", *International Journal of Computer Networks and Communications Security, 4*(6), June 2016, ss.165-176.

[12] D. Maimon, A. Fukuda, S. Hinton, O. Babko-Malaya, and R. Cathey, "On the relevance of social media platforms in predicting the volume and patterns of web defacement attacks", In *EBCS Proceedings IEEE International Conference on Big Data*, 2017, ss. 4668-4673.

[13] G. Kirwan and A. Power, *The Psychology of Cyber Crime: Concepts and Principles*, Pennyslvania, Philadelphia, USA: IGI Global Press, 2012.

[14] G. Kirwan and A. Power, *Cybercrime: The Psychology of Online Offenders*, New York, NY, USA: Cambridge University Press, 2013.

[15] M. P. Aiken, C. McMahon, C. Haughton, L. O'Neill, and E. O'Carrol, "A Consideration of the social impact of cybercrime: Examples from hacking, piracy, and child abuse material online", *Contemporary Social Science*,11(4), 2015, ss. 373-391.

[16] T. J. Holt, E. R. Leukfeldt, S. Van De Weijer, "An Examination of motivation and routine activity theory to account for cyberattacks against dutch web sites", *Criminal Justice and Behavior*, 47(4), 2020, ss. 487-505.

[17] S. Banerjee, T. Swearingen, R. Shillair, J. M. Bauer, T. J. Holt, and A. Ross, "Using machine learning to examine cyberattack motivations on web defacement data", *Social Science Computer Review 40*, 4(2022), ss. 914-932.

[18] J. Lee, M. Azamfar, J. Singh, and S. Siahpour, "Integration of digital twin and deep learning in cyber-physical systems: Towards smart manufacturing", *IET Collaborative Intelligent Manufacturing, March 2020*, 2(1), ss.34-36.

[19] F. Maggi, M. Balduzzi, R. Flores, L. Gu, and V. Ciancaglini, "Investigating web defacement campaigns at large". In *Proceedings of the Asia Conference on Computer and Communications Security (ASIACCS), Association for Computing Machinery (ACM),* New York, USA, 2018, ss. 443-456.

[20] T. Kanti, V. Richariya, and V. Richariya, "Implementing a web browser with web defacement detection techniques", *World of Computer Science and Information Technology Journal (WCSIT),* 1(7), 2011, ss. 307-310.

[21] J. Nazario, "Politically motivated denial of service attacks", in *The Virtual Battlefield,* C. Czosseck and K. Geers, Eds, Amsterdam, The Netherlands: IOS Press, 2009, ss.163-181.

[22] D. Cid, "More than 162,000 wordpress sites used for distributed denial of service attack, *Sucuri Blog*, [Online], https://blog.sucuri.net/2014/03/more-than-162000-wordpress-sites-used-for-distributed-denial-of-service-attack.html (Erişim Tarihi: Mayıs. 15, 2022).

[23] D. Kopp, M. Wichtlhuber, I. Poese, J. Santanna, O. Hohlfeld, and C Dietzel, "DDoS hide & seek: On the effectiveness of a booter services takedown", In *Proceedings of the ACM Internet Measurement Conference (IMC), Association for Computing Machinery (ACM),* New York, USA, 2019, ss. 65-72.

[24] D. R. Thomas, R. Clayton, A. R. Beresford, "1000 Days of udp amplification DDoS attacks", In *Proceedings of the APWG Symposium on Electronic Crime Research (eCrime),* 2017, ss.79-84.

[25] D. Canali and D. Balzarotti, "Behind the scenes of online attacks: An analysis of exploitation behaviors on the web", *20th Annual Network & Distributed System Security Symposium (NDSS 2013), Feb 2013, S*an Diego, USA, 2013, ss.n/a. hal-00799082

[26] T. J. Holt, "The Attack dynamics of political and religiously motivated hackers", in *Cyber Infrastructure Protection,* T. Saadawi and L. Jordan Eds, New York, USA: Strategic Studies Institute, 2009, ss.161-183.

[27] A.V. Vu, D.D. Thomas, B. Collier, A. Hutchings, R. Clayton, and R. Anderson, "Getting bored of cyberwar: Exploring the role of civilian hacktivists in the Russia-Ukraine conflict", arXiv:2208.10629v4 [cs.CR],

[28] D. Jaquet-Chiffelle and M. Loi, "Ethical and unethical hacking". in M, Christen., B. Gordijn, M. Loi, Eds, *The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology*, vol 21, 2021, ss.1-6, New York, USA: Springer-Verlag, Cham.

[29] A. Moneva, E. R. Leukfeldt, S.V.D. Weijer, and F. Miró-Llinares, "Repeat victimization by website defacement: An Empirical test of premises from an environmental criminology perspective", *Computers in Human Behavior*, *126* (2022), ss.1-11.

[30] S.V.D. Weijer, T. J. Holt, and E. R. Leukfeldt, "Heterogeneity in trajectories of cybercriminals: a longitudinal analyses of web defacements, *Computers in Human Behavior Reports, 4*(2021), 100113, ss. 1-10.

[31] G. Davanzo, E. Medvet, and A Bartoli, "Anomaly detection techniques for a web defacement monitoring service", *Expert Systems With Applications, 38*(10), ss.12521/12530, 2011.

[32] R. A. Shweder, "Why Cultural Psychology", *Ethos, 27*(1), 1999, ss.62-73.

[33] M. Minkov, *Cultural Differences in a Globalizing World*, Bingley, Plymouth, UK: Emerald Group Publishing, 2011.

[34] G. Hofstede, G. J. Hofstede, M. Minkov, *Cultures and Organizations,* New York, NY, USA: McGraw-Hill Publishing, 2010.

[35] C. D. Guss and D. Dorner, "Cultural differences in dynamic decisionmaking strategies in a non-linear, time-delayed task", *Cogn. Sys. Res.,12*(3), 2011, ss.365-376.

[36] C. Sample, J. Cowley, and S. Hutchinson, "Cultural exploration of attack vector preferences for self-identified attackers", *11th International Conference on Research Challenges in Information Science (RCIS),* Brighton, UK, 2017, ss. 305-314, doi: 10.1109/RCIS.2017.7956551.

[37] K. W. Ooi, S.H. Kim, Q. H. Wang, and K. L. Hui, "Do hackers seek variety? An empirical analysis of website defacements", In *International Conference on Information Systems, ICIS,* vol.1, AIS/ICIS Administrative Office, 2011, ss. 824-833.

[38] M. Romagna and N. J. Van den Hout, "Hacktivism and website defacement motivations, capabilities and potential threats", *27th Virus Bulletin International Conference,* October 2017, vol.1, 2017, ss.1-10.

[39] O. E. M. Mondragón, A. F. M. Arcos, C. Urcuqui, and A. N. Cavadid, "Security control for website defacement", *Sistemas & Telemática*, *15*(41), 2017, ss. 45-55, doi: 110.18046/syt.v15i41.2442. (Erişim Tarihi: May. 4, 2022).

[40] E. Sorio, A. Bartoli, and E. Medvet, "Detection of hidden fraudulent urls within trusted sites using lexical features", *2013 International Conference on Availability, Reliability and Security*, IEEE, 2013, ss. 242-247, doi: 10.1109/ARES.2013.31. (Erişim Tarihi: Mayıs. 4, 2022).

[41] D. Stuttard and M. Pinto, *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*, Hoboken, NJ, USA: John Wiley & Sons, 2011.

[42] S. Gupta and L. Sharma, "Exploitation of cross-site scripting (XSS) vulnerability on real world web applications and its defense", *International Journal of Computer Applications (IJCA),* 2012, ss.28-33.

[43] S. Gupta and B. B. Gupta, "BDS: Browser dependent xss sanitizer", In *Book on Cloud-Based Databases with Biometric Applications*, IGI-Global's Advances in Information Security, Privacy, and Ethics (AISPE) Series, 2014, ss.174-191, Pennyslvania, Philadelphia, USA: IGI Global Press.

[44] S. Gupta and B. B. Gupta, "PHP-Sensor: A Prototype Method to Discover Workflow Violation and XSS Vulnerabilities in PHP Web Applications". In *Proceedings of the 12th ACM*

International Conference on Computing Frontiers. ACM. FISP'15, May 18-21, Ischia, Italy, 2015, ss.1-8, doi: 10.1145/2742854.2745719. (Erişim Tarihi: Mayıs 7, 2022).

[45] A. Barth, C. Jackson, and J. C. Mitchell, "Robust defenses for cross-site request forgery". In *Proceedings of The 15th ACM Conference on Computer and Communications Security*, 2008, ss.75-88.

[46] İ. Üzüm and Ö. Can, "An anomaly detection system proposal to ensure ınformation security for file ıntegrations", In *2018 26th Signal Processing and Communications Applications Conference (SIU)*, IEEE, 2018, ss.1-4.

[47] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, "Denial-of-service attack-detection techniques", *IEEE Internet Computing*, *10*(1), 2006, ss. 82-89.

[48] N. Borisov, G. Danezis, P. Mittal, and P. Tabriz, "Denial of service or denial of security?", In *Proceedings of The 14th ACM Conference on Computer and Communications Security*, 2007, ss. 92-102.

[49] Q. Gu and P. Liu, "Denial of service attacks", *Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications*, vol.*3*, 2007, ss.454-468.

[50] S. Liu, X. P. Liu, and A. El Saddik, "Denial-of-service (dos) attacks on load frequency control in smart grids", In *2013 IEEE Pes Innovative Smart Grid Technologies Conference (ISGT)*, IEEE, 2013, ss.1-6.

[51] E. Moradian and A. Håkansson, "Possible attacks on xml web services", *IJCSNS International Journal of Computer Science and Network Security*, 6(1B), 2006, ss.154-170.

[52] C. Gupta, R. K. Singh, A. K. Mohapatra, "A Survey and classification of xml based attacks on web applications", *Information Security Journal: A Global Perspective*, 29(4), 2020, ss.183-198.

[53] E. Karaarslan, T. Tuğlular, and H. Şengonca, "Web saldırı saptama ve engelleme sistemi temelleri", *Türkiye Bilişim Vakfi Bilgisayar Bilimleri ve Mühendisliği Dergisi,* 2(1), 2016, ss.1-8.

[54] F. Kargl, J. Maier, and M. Weber, "Protecting web servers from distributed denial of service attacks". In *Proceedings of the 10th International Conference on World Wide Web, WWW10,* 1-5 May 2001, Hong Kong, 2001 ss. 514-524, doi: 10.1145/371920.372148. (Erişim Tarihi: Mayıs. 7, 2022).

[55] M. Jensen., N. Gruschka., R., Herkenhöner, "A Survey of attacks on web services: classification and countermeasures", *Computer Science-Research and Development,* 24, 2009, ss.185-197.

[56] B. Sterling, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, Penguin (Books), Baltimore, MD, USA: Mass Market Paperback, 1993.

[57] S. Levy, *Hackers: Heroes of the Computer Revolution*, Penguin (Books), Baltimore, MD, USA: 1984.

[58] S. Lysonski and S. Durvasula, "Digital piracy of mp3s: Consumer and ethical predispositions", *Journal of Consumer Marketing*, 25(3), 2008, ss.167-178, doi: 10.1108/07363760810870662. (Erişim Tarihi: Mayıs. 6, 2022).

[59] D. J. Gunkel, "Editorial: Introduction to hacking and hacktivism", *New Media & Society*, 7(5), 2005, ss. 595-597, doi: 10.1177/1461444805056007. (Erişim Tarihi: Mayıs. 6, 2022).

[60] J. Suler, "The Online disinhibition effect", *Cyberpsychology & Behavior: The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society,* 7(3), 2004, ss.321-326, doi: 10.1089/1094931041291295. (Erişim Tarihi: Mayıs. 4, 2022).

[61] T. T. Moores and J.C.J. Chang, "Ethical Decision Making in Software Piracy: Initial Development and Test of A Four-Component Model", *MIS Quarterly,* 30(1), 2006, ss. 167-180. [online] http://dl.acm.org/citation.cfm?id=2017284.2017294 (Erişim Tarihi: Mayıs. 2, 2022).

[62] M. Warren, "The Ethics of the hacker taggers: The New Generation of Hackers", In. *Proceedings of The Tenth International Conference Living, Working and Learning Beyond Technology, ETHICOMP 2008*, T.W. Bynum, M. Calzarossa, I. D. Lotto & S. Rogerson (Eds.), University of Pavia, 24-26 September 2008, Mantua, Italy, 2008, ss.787-793.

[63] M. Warren and S. Leitch, "Hacker taggers: A New type of hackers", *Information Systems Frontiers*, 2009, ss.425-431, doi: 10.1007/s10796-009-9203y. (Erişim Tarihi: Mayıs. 6, 2022).

[64] M. C. Calzarossa, I. D. Lotto, and S. Rogerson, "Ethics and Information Systems -Guest Editors' Introduction". *Inf Syst Front* 12, 357-359, 2010, ss.357-359, doi: 10.1007/s10796-009-9198-4. (Erişim Tarihi: Mayıs. 8, 2022).

[65] S. Furnell, "Hackers, viruses and malicious software", in *Handbook of Internet Crime*, Y. Jewkes and M. Yar, Eds, Cullompton, UK: Willan, 2009, ss.173-193.

[66] H. J. Woo, Y. Kim, J. Dominick, "Hackers: Militant or merry pranksters? A Content analysis of deface web pages", *Media Psychology,* 6, 2004, ss.63-82.

[67] A.K. Jain, S.R. Sahoo, and J. Kaubiyal, "Online social networks security and privacy: comprehensive review and analysis". *Complex Intell. Syst. 7*, (2021), ss. 2157-2177, doi: 10.1007/s40747-021-00409-7.

[68] A. Weber, "The Council of Europe's convention on cybercrime", *Berkeley Technology Law Journal*, 18(1), Annual Review of Law and Technology, 2003, ss.425-444.

[69] M. Gercke, *Understanding Cybercrime. A Guide for Developing Countries*, 2nd Ed, Geneva, Switzerland, ITU, 2011.

[70] Tonya L. Putnam and D. D. Elliott, "International Responses to Cyber Crime", A. Sofaer and S. Goodman, Ed, *Transnational Dimension of Cyber Crime and Terrorism*, 2001, ss. 35-67, Stanford California, USA: Stanford University Hoover Institution press.

[71] O. S. Kerr, "Searches and seizures in a digital world", *Harvard Law Review*, 119(2), 2005, ss.531-585, Available at SSRN: https://ssrn.com/abstract=697541

[72] S. D. Moitra, "Developing policies for cybercrime", *13 Eur. J. Crime Crim. L. & Crim. Just*, 2005, ss. 435-464.

[73] H. Sınar, *Avrupa Konseyi Siber Suç Sözleşmesi Üzerine Bir Deneme*, Prof. Dr. Çetin Özek Armağanı, 2004, ss.765-300.

[74] J. Clough, *Principles of Cybercrime*, New York, NY, USA: Cambridge University Press, 2010.

[75] Council of Europe, *Convention on Cybercrime*, ETS (European Treaty Series), No:185, 2001.

[76] ITU, "ITU_T X.1205 Sayılı tavsiye kararı, siber güvenliğe genel bakış", 2008.

[77] A. Karagülmez, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, 4th Ed., İstanbul, Türkiye: Seçkin Yayıncılık, 2013.

[78] H. Akıncı, A. E. Alıç ve C. Er, "Türk ceza kanunu ve bilişim suçları", *İnternet ve Hukuk*, Y. M. Atamer, Ed, İstanbul, Türkiye: İstanbul Bilgi Üniversitesi Yayınları, 2004.

[79] Ö. Uçkan and Y. Beceni, "Bilişim-iletişim teknolojileri ve ceza hukuku*", İnternet ve Hukuk*, Y. M. Atamer, Ed, İstanbul, Türkiye: İstanbul Bilgi Üniversitesi Yayınları, 2004.

[80] L. Kurt, *Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanundaki Uygulaması*, 1st Ed, Ankara, Türkiye: Seçkin Yayıncılık, 2005.

[81] Resmi Gazete, "İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun, 5651 Sayılı Kanun", Kabul Tarihi:4/5/2007, Resmi Gazete, 23/5/2007, Sayı:26530: Tertip:5, Cilt:46. 2007.

[82] Zone-H, "Zone-H website main page", http://www.zone-h.org/ (Erişim Tarihi: Ekim. 1, 2022).

[83] Zone-H, "Monthly attack statistics for 01/22-10/22", http://www.zone-h.org/stats/ymd (Erişim Tarihi: Ekim. 31, 2022).

[84] Zone-H, "Annual attack statistics for 2015-2022", http://www.zone-h.org/stats/ymd (Erişim Tarihi: Ekim. 31, 2022).

[85] Zone-H, "Example page mirroring-tagging section of Hmei7 coded hacker", http://www.zone-h.org/archive/notifier=Hmei7 (Erişim Tarihi: Ekim. 31, 2022).

[86] Zone-H, "Example page mirroring-tagging section of hacker code 0x1998", http://www.zone-h.org/mirror/id/39410678 (Erişim Tarihi: Ekim. 31, 2022).

[87] Zone-H, "Example page mirroring-tagging section of Ramil Feyziyev coded hacker", http://www.zone-h.org/mirror/id/40641580 (Erişim Tarihi: Ekim 31, 2022).

[88] Zone-H, "Example page mirroring tagging cross section of Yodo coded hacker", http://www.zone-h.org/mirror/id/40626693 (Erişim Tarihi: Ekim. 31, 2022).