İnternet Sitelerine Yapılan Siber Saldırılar: 2015 Yılı Türk Kamu Siteleri İncelemesi

Cyber Attacks to Web Sites: Examination of Government Web Sites of Turkey in 2015

Hüseyin ÇAKIR[*], Nursel YALÇIN[**] ve Mehmet Serkan KILIÇ[***]

Öz

Kamunun internet ortamında sunduğu hizmetlerin artması, siber saldırı risklerini de beraberinde getirmektedir. Günümüzde kamu kurumlarına ait internet sitelerine yönelik yapılan siber saldırılar hızlı bir şekilde artmaktadır. Bu çalışmada, 2015 yılında Türkiye'de kamuya ait ".gov.tr" uzantılı internet sitelerine yapılan siber saldırıların (bütünlük ihlalleri) değerlendirilmesi amacıyla Zone-H internet sitesinde yer alan toplam 848 saldırı kaydı incelenmiştir. Gerçekleştirilen saldırılar; aylara göre saldırı bilgileri, ana sayfa saldırı bilgileri, geçmiş saldırı bilgileri, sunuculara ait bilgiler ve saldırganlara ait bilgiler olmak üzere beş açıdan analiz edilmiştir. Zone-H kayıtlarında yer alan takma isimlere, mesajlara, resim ve video paylaşımlarına göre saldırıların 25 farklı ülkeden toplam 131 farklı bilgisayar korsanı/bilgisayar korsanları grubu tarafından gerçekleştirildiği anlaşılmıştır. Bununla beraber saldırıların %70'inin Türkiye merkezli olduğu ve saldırıya uğrayan internet sitelerinin %35'inin geçmişte de saldırıya uğradığı görülmüştür.

Anahtar Kelimeler*: Bütünlük İhlali, Bilgisayar Korsanı, Siber Saldırı, Zone-H.*

[*] Yrd.Doç.Dr., Gazi Üniversitesi, Bilişim Enstitüsü, Adli Bilişim Anabilim Dalı, e-posta: hcakir@gazi.edu.tr.

[**] Yrd.Doç.Dr., Gazi Üniversitesi, Gazi Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, e-posta: nursel_yalcin@hotmail.com.

[***] Doktora Öğrencisi, Gazi Üniversitesi, Bilişim Enstitüsü, Bilişim Sistemleri Anabilim Dalı, e-posta: mserkanklc@hotmail.com.

Abstract

The increase in the internet services provided by government brings the risks of cyber attacks. Today, the cyber attacks to the web sites of the government institutions have increased rapidly. In this study, 848 cyber attack records in Zone-H web site have been examined to evaluate the cyber attacks (integrity violations) to Turkish government web sites with ".gov.tr" extensions. The attacks, which were performed, have been analyzed through five different perspectives as attack information by months, information of homepage attacks, information about past attacks, information about servers and information about attackers. According to fake names, messages, and sharing of pictures and videos in Zone-H records, it has been made clear that the cyber attacks have been performed by 131 different hackers or hacker groups from 25 different countries. In addition to this, it has also been seen that 70% of attacks are of Turkey origin and 35% of web sites, which were attacked, had been attacked previously.

Keywords: *Integrity Violation, Hacker, Cyber Attacks, Zone-H.*

1. Giriş

Ülkemizde 2008 yılında altı milyon civarında olan geniş bant internet abonesi sayısı, 2015 yılı ikinci çeyrek sonu itibarıyla 44,3 milyonu aşmıştır.[1] İnternetin yaygınlaşması ile beraber alışverişten, akademik çalışmalara kadar birçok iş ve işlem internet ortamında hızlı ve kolay bir şekilde gerçekleştirilmektedir.

Yüksek hızlı bilgisayar teknolojisi, internet, televizyon, ATM, cep telefonu, uydu teknolojisi, dijital kayıt sistemleri, robotlar ve lazer teknolojisi insan hayatında her gün daha etkin bir şekilde kullanılmış ve devlete ait işlemlerde de kullanılır hale gelmiştir.[2] Bilgi ve iletişim

[1] ***BTK Üç Aylık Pazar Verileri Raporu: 2015 Yılı 2. Çeyrek***, Bilgi Teknolojileri ve İletişim Kurumu, Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı, Ankara, 2015, s. 9.

[2] Özgür Sayar, Türkiye'de ve Dünyada Elektronik Devlet Uygulamaları Bağlamında Risk Faktörleri, Beykent Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2007, s. 9.

teknolojilerindeki gelişmelere paralel olarak kamu kurumları tarafından oluşturulan internet siteleri; idarelere zaman, yer, verimlilik ve benzeri bakımlardan fayda sağlamaktadır. Oluşturulan internet siteleriyle etkin, verimli, hesap verebilir, vatandaş beyanına güvenen ve şeffaf bir kamu yönetimi oluşturmak, kamu hizmetlerinin hızlı, kaliteli, basitleştirilmiş ve düşük maliyetli bir şekilde yerine getirilmesini sağlamak amaçlanmaktadır.[3] Bu amaçla ülkeler gelişmişlik düzeylerine göre kamu hizmetlerini internet ortamına aktarmakta ve vatandaşlarına hızlı ve kaliteli hizmetler sunmaktadır.

Kamu kurumları tarafından oluşturulan internet siteleri ve sunulan hizmetlerin vatandaşlar üzerinde pozitif etkisi bulunmakla beraber, sunulan hizmetin kesintisiz ve güvenli bir şekilde sağlanması önemli bir zorluktur. Çeşitli sebeplerle başta kamu internet siteleri olmak üzere ülkede stratejik olarak önemli görülen internet sitelerine yapılan siber saldırılar, itibar kaybına ve hizmetlerin aksamasına neden olmaktadır.

İnternet sitelerine yönelik saldırılar; sitenin politik ve sosyal mesaj vermek amaçlı ele geçirilmesi ve Hizmet Engelleme Saldırısı (*Denial of Service Attack*-DoS) saldırısı ile siteye erişimin engellenmesi olmak üzere iki şekilde gerçekleştirilmektedir.[4] Birçok bilgisayar sahibi, bilgisayarlarının zombi olduğunun (ele geçirildiğinin) veya Dağıtık Hizmet Aksatma (*Distributed Denial of Service*-DDoS) saldırısı yaptığının farkında olmamakta ve bilgisayarlarının hedef internet sitesine arka planda bağlantı kurmaya çalıştığını bilmemektedir.[5] Diğer taraftan, devlet politikaları sebebi ile planlı şekilde DDoS saldırısı yapıldığı durumlar da bulunmaktadır. Kullanıcılar çeşitli platformlar aracılığıyla

(Yayımlanmamış Yüksek Lisans Tezi).

[3] Ali Haydar Doğu, "İdarelerin İnternet Sitelerinden Doğan Sorumlulukları", ***18. Türkiye'de İnternet Konferansı Bildirileri,*** 9-11 Aralık 2013, İstanbul Üniversitesi, İstanbul, 2013, s. 2.

[4] Dorothy E. Denning,"Cyber Conflict as an Emergent Social Phenomenon", (Ed: Holt, T.J. ve Schell, B.H.), ***Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications,*** IGI Global Press, PA, ABD, 2011, 170-186, s. 173.

[5] Mahruze Kara, Siber Saldırılar - Siber Savaşlar ve Etkileri, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2013, s. 38. (Yayımlanmamış Yüksek Lisans Tezi).

örgütlenerek ve kendi rızalarıyla bilgisayarlarına kurdukları programlar ile DDoS saldırılarının bir parçası olmakta ve yapılan siber saldırı eylemini desteklemektedir.

İnternet sitelerinde bulunan açıklıklar veya sosyal mühendislik yöntemleri ile internet sitelerine yetkisiz şekilde erişilmesi, başta ana sayfa olmak üzere sitenin sayfalarına mesajlar bırakılması ve özel verilerin (kişisel veri, gizli veri) ele geçirilmesi diğer bir yaygın siber saldırı yöntemidir. Bilgisayar korsanları tarafından farklı motivasyonlarla gerçekleştirilen bu saldırılar; toplum tarafından farklı algılanmakta ve farklı tepkiler verilmesine sebep olmaktadır.

Bir internet sitesine yapılan saldırı ve siteye bırakılan mesajlar, ziyaretçiler üzerinde negatif etki bırakması nedeniyle ticari olarak prestij kaybına neden olmakta ve iş dünyası açısından siber saldırılar önemli bir tehdit olarak görülmektedir.[6] Toplumun bir kesimi tarafından ise aynı eylem bir konuya dikkat çekildiği gerekçesi ile alkışlanabilmektedir. Jurgenson benzer şekilde, politik veri sızma ile dünya gündemine gelen Wikileaks ve Julian Assange hakkında siber-liberalist/siber-anarşist tanımlaması konusunda toplumda tartışmalar yaşandığına[7] dikkat çekmektedir. Kimliklerin kolayca gizlenebildiği ve iz sürmenin son derece zor olduğu siber alanda rakip veya düşman olarak görülen devletlere zarar verici nitelikte siber saldırıları destekleyen devletler bulunmaktadır.[8] Bu durum siber saldırıların çok farklı motivasyonlarla bir silah olarak kullanıldığını göstermektedir.

Siber saldırıların oluşturduğu etki ve tahribattan dolayı, tespiti önemli bir konu olmuştur ve bu yönde akademik çalışmalar ağırlık

---

[6] Tushar Kanti et. al., "Implementation of an Efficient Web Defacement Detection Technique And Spotting Exact Defacement Location Using Diff Algorithm", ***International Journal of Emerging Technology and Advanced Engineering***, 2012, 2 (3), 252-256, p. 252.

[7] Nathan Jurgenson, "Liquid Information Leaks", ***International Journal of Communication***, 2014, 8, 2651–2665, s. 2657.

[8] Mehmet Nesip Öğün ve Adem Kaya, "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler", ***Güvenlik Stratejileri Dergisi***, 2013, 18, 145-181, s. 167.

kazanmıştır. Kanti vd. tarafından yapılan bir çalışmada, tahrif edilmiş internet sitesi sayfalarının tespiti amacıyla internet tarayıcıları için geliştirilen algoritma ile ziyaret edilen internet sayfalarının karma değerlerinin düzenli olarak hesaplanması, karşılaştırılması ve farklılık durumunda uyarı vermesi amaçlanmıştır.[9] Borgolte vd. tarafından yapılan çalışmada ise, saldırıya uğrayan internet sitelerine bilgisayar korsanları tarafından mesaj bırakılmasından hareketle internet sayfalarına ait ekran görüntülerinin alınması, resim tabanlı analiz edilmesi ve sitenin saldırıya uğrayıp uğramadığının tespiti amaçlanmıştır.[10] Saldırıya uğrayan internet sitelerinin en kısa sürede tespit edilmesi ihtiyacı, saldırıların toplum üzerinde oluşturacağı negatif etkinin en aza indirilmesi isteğidir. Bu açıdan bilişim teknolojilerine olan bağımlılığın devam ettiği sürece "siber saldırı" ve "siber güvenlik" konularının kamuoyunda önemli yer tutacağı değerlendirilmektedir.

Bu çalışmada, gelişen ve kullanım alanı yaygınlaşan bilişim teknolojileri ile beraber internet sitelerine yapılan siber saldırılar Türkiye özelinde ele alınmıştır. Birçok devlet hizmetinin elektronik ortamda vatandaşlara sunulduğu ülkemizde, devlete ait internet sitelerine yapılan saldırılar incelenerek farklı açılardan değerlendirmelerde bulunulmuştur. Açık kaynaklardan elde edilen veriler üzerinde yapılan bilimsel değerlendirmeler ile ülkemizin siber güvenlik politikalarına katkı sağlanması amaçlanmaktadır.

Çalışmanın ilk bölümünde, siber güvenlik ihlalleri erişilebilirlik, bütünlük ve gizlilik açılarından ele alınarak bilgi verilmiştir. "Bilgisayar Korsanı ve Bilgisayar Korsanlığı Kültürü" isimli ikinci bölümde bilgisayar korsanlığı ve bilgisayar korsanı kavramları hakkında genel bilgiler verildikten sonra bilgisayar korsanlığı kültüründe sistem kırıcılar, bilgisayar korsanlığı kültüründe gizlilik, bilgisayar korsanlığı kültüründe aleniyet ve bilgisayar korsanlığı kültüründe motivasyon alt başlıkları

[9] Tushar Kanti et. al., a.g.m., s. 253.
[10] Kevin Borgolte et. al., Meerkat: Detecting Website Defacements Through Image-Based Object Recognition, ***24th USENIX Security Symposium***, 12-14 August 2015, Washington, DC, USA, 2015, p. 545.

altında bilgisayar korsanlığı kültürü konusu irdelenmiştir. Çalışmanın "Türkiye'de Kamuya Ait İnternet Sitelerine Yapılan Siber Saldırılar" isimli üçüncü bölümünde ise 2015 yılında Türk kamu sitelerine yönelik yapılan siber saldırılar ele alınmıştır. Çalışmaya konu veriler açık kaynak üzerinde Zone-H internet sitesinde (www.zone-h.org) yer alan ".gov.tr" uzantılı siber saldırı kayıtları esas alınarak oluşturulmuştur. Buna göre, Zone-H internet sitesinde yer alan 2015 yılına ait toplam 848 saldırı kaydı; aylara göre saldırı bilgileri, ana sayfa saldırı bilgileri, geçmiş saldırı bilgileri, sunuculara ait bilgiler ve saldırganlara ait bilgiler olmak üzere beş açıdan analiz edilmiştir. Özellikle saldırganlara ait bilgiler isimli alt başlıkta, internet sitelerine bırakılan mesajlar incelenerek saldırganlara ait ülke bilgileri tespit edilmeye çalışılmıştır. Çalışmanın son bölümünde ise genel bir değerlendirme yapılarak çalışma boyunca ulaşılan sonuçlara yer verilmiştir.

2. Siber Güvenlik İhlalleri

Siber güvenlik; sanal ortamda gerçekleşen saldırılar sonucu bilişim sistemlerinin zarar görmemesi, yetkisiz bir şekilde sayısal verilere ulaşılmaması ve zarar verilmemesi ile yaşanan siber saldırılar sebebiyle kamuoyunda korku ve panik oluşmaması için alınması gereken önlemlerdir. Bu önlemler, vatandaşların bilinçlendirilmesinden ve kişisel bilgisayar güvenliğinin sağlanmasından ulusal siber olaylara müdahale ekiplerinin oluşturulmasına kadar bir dizi alt başlıklardan oluşmaktadır.

İnternet üzerindeki işlemlerin ekonomik değerinin artması, internetin anonim yapısı, saldırı araçlarının ucuzlaması ve bunlara erişimin kolaylaşması, suçlular arasındaki iş birliğinin kolaylaşması ve artması gibi nedenlerle önümüzdeki dönemde yeni suç türlerinin ortaya çıkması ve siber suçlarda artışın devam etmesi beklenmektedir.[11] Siber saldırıların engellenmesi ve güvenliğin sağlanması ise uluslararası kabul görmüş üç temel güvenlik standardı olan erişilebilirlik, bütünlük ve gizliliğin korunması ve ihlal edilmemesinin sağlanmasıdır.

[11] ***2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı***, Kalkınma Bakanlığı, Bilgi Toplumu Dairesi Başkanlığı, s.29.

Erişilebilirlik, bir bilgiye ulaşmaya yetkili olan herkesin gerektiğinde o bilgiye erişiminin mümkün olması; bütünlük, bir bilginin hiçbir şekilde değiştirilmemiş olması; gizlilik ise bir bilgiye erişim hakkı olan kişilerin belirlenmesi ve diğer kişilerin bilgiye ulaşmasını engellemesidir.[12] Bu üç temel güvenlik öğesinden herhangi birinin zarar görmesi durumunda güvenlik zafiyeti oluşmaktadır. Bilgi güvenliği kurumlar ve bireyler için vazgeçilmez ve değerli bir varlık olan bilginin korunması için gerekmektedir.[13]

2.1. Erişilebilirlik İhlali

Türk Dil Kurumu sözlüğünde "genel ağda bir sayfanın ulaşılabilir olması"[14] şeklinde tanımlanan erişilebilirlik, hukuki sınırlamalar saklı kalmak üzere aynen seyahat ve haberleşme özgürlüğü gibi bireylerin istediği internet sitesine bağlanabilme, ulaşabilme ve ziyaret edebilme özgürlüğüdür.

Ülkemizde internet siteleri erişiminin engellenmesi başta 5651 Sayılı Kanun olmak üzere yasal mevzuatlarla düzenlenmiştir. Buna göre, 5651 Sayılı Kanunda belirtilen katalog suçlar kapsamında verilen erişimin engellenmesi kararları, kararı veren hâkim, mahkeme veya cumhuriyet savcısı tarafından gereği yapılmak üzere Bilgi Teknolojileri ve İletişim Kurumu'na (BTK) gönderilmekte ve kararlar BTK tarafından yerine getirilmektedir. Ayrıca anılan kanunun sekizinci maddesinde sayılan suçların oluşması durumunda ilgili içerik veya yer sağlayıcı yurtdışında ise BTK tarafından resen erişimin engellenmesi yapılabilmektedir. Hukuki sınırlamalar haricinde, bir internet sitesine yasadışı müdahaleler ile de erişim engellenebilmektedir.

DDoS, en basit saldırı tipi olduğundan siber saldırılarda yoğun olarak kullanılmaktadır. Saldırının amacı, sistemi durdurarak prestij ve

[12] Emine İlçin Tuğ vd., "Bilişim Güvenliği Tedbirleri ve TKDK Kurumunda Uygulama Örneği", ***Bilişim Teknolojileri Dergisi,*** 2014, 7 (1), 11-18, s. 12.
[13] Hafize Keser ve Can Güldüren, "Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme Çalışması", ***Kastamonu Eğitim Dergisi,*** 2013, 23 (3), 1167-1184, s. 1168.
[14] Türk Dil Kurumu İnternet Sitesi, www.tdk.gov.tr, (Erişim Tarihi: 04.12.2015).

maddi kayıp sağlamaktır. Bilgisayar korsanlığı eylemciliği grupların genellikle kullandıkları bu yöntem, rahatsız edici ve maddi zararlara yol açan bir unsurdur.[15] Devletler arasında yaşanan siyasi gerilimlerin yansıması olarak siber dünyada gerçekleşen saldırılarda da karşı tarafa zarar vermek ve ülke güvenliğini sağlayan yönetimlerin itibarını sarsmak için bu tür yöntemler kullanılmaktadır.[16] Yaşanan erişilebilirlik ihlallerinin çoğunluğunda internet sitesi içeriğine zarar verilmemekte ve kullanıcıların siteye olan erişimleri bir süreliğine engellenmektedir.

2.2. Bütünlük İhlali

İnternet sitelerinin başta sistem açıklıkları olmak üzere çeşitli yöntemler kullanılarak tamamının veya bir bölümünün içeriğine ulaşılarak değişikliklerde bulunulması durumunda, bütünlük ihlali oluşmaktadır. İnternet sitesinin bilgisayar korsanlığına maruz kalması olarak bilinen bu ihlalde siteye olan erişimin engellenmesinin yanı sıra içeriğinin değiştirilmesi ve zarar verilmesi durumu da söz konusudur.

İnternet sitelerine yönelik yapılan en önemli iki saldırı yönteminin Yapılandırılmış Sorgu Dili (*Structured Query Language*-SQL) Girişi ve Çapraz Site Betik (*Cross-Site Scripting*-XSS) Saldırısı olduğu hususu *Open Web Application Security Project* (OWASP) tarafından açıklanmıştır. İnternet sayfalarında bulunan veri girişi formları aracılığı ile zararlı kodların çalıştırıldığı saldırılarda[17] internet sitesi açıklıkları kullanılmakta ve site bütünlüğüne zarar verilmektedir. Kullanılan açıklıklar ile birçok saldırı siber ortamın sadece görünen yüzü olan web sitelerinin ana sayfalarına karşı gerçekleşmekte ve aslında ciddi zararlar oluşturmamaktadır.[18] Bununla birlikte, siteye bırakılan mesajlar

[15] Mahruze Kara, ***a.g.e.***, s. 38.
[16] Muharrem Gürkaynak ve Adem Ali İren, "Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler", ***Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi***, 2011, 16 (2), 263-279, s. 271.
[17] Sandra Sarasan, "Detection and Prevention of Web Application Security Attacks**"**, ***International Journal of Advanced Electrical and Electronics Engineering***, 2013, 2 (3), 29-34, s. 29.
[18] Mehmet Nesip Öğün ve Adem Kaya, a.g.m., s. 171.

sebebiyle maddi kazanç ve imaj kaybı söz konusu olmaktadır.

2015 yılında yapılan bir araştırmada; internet site saldırılarının %24'ünde bırakılan mesajlar bir gün içinde kaldırılırken, %50'sinde bırakılan mesajların bir hafta içinde kaldırıldığı anlaşılmıştır. Bu durum, şirket sahiplerinin web site koruma ve saldırı tespit sistemlerine yeteri kadar yatırım yapmadığını göstermektedir.[19] Saldırı sonrası en kısa sürede internet sitelerinin eski haline getirilerek imaj ve prestij kaybı yaşanmaması amacıyla, site sahiplerinin ek harcamalar yapması ve gerekli güvenlik tedbirlerini alması gerekmektedir.

2.3. Gizlilik İhlali

Bilginin yetkisiz kişilerin eline geçmesi olarak tanımlanabilecek gizlilik ihlali; internet sitesine yetkisiz şekilde erişen ve bütünlük ihlali yapan saldırgan tarafından sunucuda bulunan ve herkese açık olmayan elektronik verilerin ele geçirilmesidir. Bu verilerin ele geçirilmesi başlı başına suç oluşturmakla beraber, verilerin maddi menfaate dönüştürülmesi veya çeşitli ortamlarda yayınlanarak alenileştirilmesi ise suçun ağırlaştırılmış hâli ve/veya başka suçların oluşması durumudur. Bu açıdan bakıldığında bilişim sisteminde yer alan veriler üzerinde hukuka aykırı birtakım işlemler gerçekleştiren kişilerin eylemi Türk Ceza Kanunu'nun (TCK) 244'üncü maddesinin ikinci fıkrası kapsamında suç teşkil etmektedir. Bu eylemin icrası ile kişinin kendine veya başkasına haksız menfaat sağlaması durumunda ise TCK 244'üncü maddesinin dördüncü fıkrasında yer alan suç oluşacaktır.

Bilgisayar korsanları, sosyal mühendislik yaparak veya internetin açıklıklarından faydalanarak sosyal uygulama ve e-posta hesaplarının şifrelerini kırabilmekte; sistemlere izinsiz sızabilmekte; ulusal ve uluslararası güvenlik sırlarına erişebilmekte ve eriştiği bilgileri çalabilmektedir.[20] Her ne kadar bazı saldırılarda hedef; kendi çıkarı değil, organizasyonların bilgi güvenliği konusundaki yetersizliklerinin

[19] Kevin Borgolte et. al., ***a.g.e.***, p. 598.
[20] Mahruze Kara, ***a.g.e.***, s. 9.

vurgulanması amacıyla kamuoyuna duyurulması[21] olsa da, yapılan saldırılar sonucu yaşanan bilgi kayıpları kurumların itibarlarını zedelemekte; güvenilirliklerini azaltmakta; pazar ve müşteri kayıplarına neden olabilmektedir.[22] Sonuç olarak, bazı uygulamaların yardımıyla basit bir şekilde ana sayfa değişikliği yapmanın ötesinde, orta seviyenin üzerindeki bilişim bilgisiyle hedef sunucuyu kontrol altına alarak yetkisiz şekilde bilgilere erişmek, gizlilik ihlalini oluşturmaktadır ve bu durum TCK'nın 243'üncü maddesinin birinci fıkrasında suç olarak düzenlenmiştir.

3. Bilgisayar Korsanı ve Bilgisayar Korsanlığı Kültürü

Bilgisayar korsanlığı kavramının ilk ortaya çıktığı yer, ABD'deki Massachusetts Institute of Technology'dir (MIT). MIT öğrencilerinin kendi aralarında yaptıkları eşek şakalarına verdikleri isim "*hack*"tir (korsanlıktır). Zamanla bilgisayar aracılığıyla yapılan şakalar için de bu isim kullanılmıştır.[23] 1988'de Clifford Stoll tarafından yazılan "Stalking The Willy Hacker" başlıklı makalede[24] bilgisayar korsanlığı ve bilgisayar korsanı terimleri ilk kez bilgisayar suçlusu anlamında kullanılmış ve takip eden yılda, Robert Tapan Morris Jr. tarafından yayılan Morris virüsü, popüler medyada bu kullanımın yaygınlaşmasını sağlamıştır.[25] Zeki insanların yaptıkları zekice şaka olarak tanımlanan "*hack*" (korsanlık) kavramı, bir süre sonra diğer insanlar üzerinde oluşan olumsuz algı ile beraber "suç" olarak görülmeye başlanmıştır.

Benzer durum ülkemiz açısından da geçerlidir. Türk Dil Kurumu (TDK), Güncel Türkçe Sözlük'te "bilgisayar korsanı" ("*hacker*") terimi

---

[21] Alexandra Whitney Samuel, Hacktivism and the Future of Political Participation, Harvard University Department of Government, Cambridge, ABD, 2004, p. 11 (Yayımlanmamış Doktora Tezi).

[22] Emine İlçin Tuğ vd., a.g.m., s. 11.

[23] Gökşin Akdeniz, "Hacker Etiği", (Der: Keleş, A.R. ve Sal, Y.), ***Hack Kültürü ve Hacktivizm: Yeni bir Siyaset Biçimi***, Alternatif Bilişim Derneği Yayını: İstanbul, 2013, 9-15, s. 9.

[24] Makale için bkz. http://pdf.textfiles.com/academics/wilyhacker.pdf, Erişim Tarihi: 20 Şubat 2017.

[25] Ufuk Eriş, Türkiye'de Kırıcı (Hacker) Kültürü, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Eskişehir, 2009, s. 64 (Yayımlanmamış Doktora Tezi).

"bilgisayar ve haberleşme teknolojileri konusundaki bilgisini gizli verilere ulaşmak, ağlar üzerinde yasal olmayan zarar verici işler yapmak için kullanan kimse" olarak tanımlanmaktadır.[26] Oysa ki, bu terimin TDK tarafından 2005 yılında "bilgisayar haberleşme teknolojileri konusunda bilgi sahibi olan, bilgisayar programlama alanında standardın üzerinde beceriye sahip bulunan ve böylece ileri düzeyde yazılımlar geliştiren kişi"[27] olarak tanımlandığı bilinmektedir. Bilgisayar korsanı ve bilgisayar korsanlığı kavramlarındaki bu anlam kaymasında, toplumsal algı ve "standardın üzerindeki bilgi ve becerinin" yetkisiz erişim faaliyetlerinde kullanılıyor olmasının payı büyüktür. Bu bağlamda bilgisayar korsanı kavramının, genel olarak bilişim sistemleri konusunda yetenekli, sistem açıklıklarını arayan ve bu açıklıklardan izinsizce sisteme sızan kişiler[28] olarak tanımlanması mümkündür. Bununla birlikte, son dönemde ortaya çıkan bilgisayar korsanlığı eylemciliği kavramı ile birlikte kavram karmaşası tekrar yaşanmakta ve bilgisayar korsanlarının suçlu mu yoksa kahraman mı oldukları tartışma konusu olmaktadır.

Bilgisayar korsanlığı kültürünü "internet erişimi özgürlüğüne karşı yapılan her türlü düzenleme, sınırlama ve sansüre karşı düşmanlık" olarak ele alan düşünceye[29] paralel olarak bilgisayar korsanı, kişisel çıkarının değil; bilginin ve daha da ötesinde denetim altına alınmamış anlamın peşinde olan kişi olarak[30] da tanımlanabilmektedir. Bilgisayar korsanlığı eylemciliği ise politik gerekçelerle temelde birey yararını güderek internet üzerinden siber saldırı, protesto ya da eylem biçiminde bireysel tepkinin siber biçim ile yer değiştirmesi olarak ifade edilmektedir.[31] Bu düşünceye

[26] Türk Dil Kurumu İnternet Sitesi, www.tdk.gov.tr, (Erişim Tarihi: 08.12.2015).
[27] Ufuk Eriş, ***a.g.e.***, s. 67.
[28] Mahruze Kara, ***a.g.e.***, s. 9.
[29] Nathan Jurgenson, a.g.m., s. 2556.
[30] Özgür Uçkan,"Hacker'lar: Viral Kültürün "Semantik Gerillalar"ı mı, Enformasyon Toplumunun Veri Hırsızları mı?", (Der: Keleş, A.R. ve Sal, Y.), ***Hack Kültürü ve Hacktivizm: Yeni bir Siyaset Biçimi***, Alternatif Bilişim Derneği Yayını: İstanbul, 2013B, 41-47, s. 46.
[31] Ceren Yegen, Dijital Aktivizmin Bir Türü Olarak Hacktivizm ve "RedHack", ***Intermedia Uluslararası Hakemli İletişim Bilimleri E-Dergisi***, 2014, 1 (1), 118-132, s. 129.

göre, bilgisayar korsanları toplum yararına sanal ortamda mücadele eden siber eylemcilerdir.

Devlet politikaları açısından bakıldığında ise, yapılan siber saldırıların terörist faaliyet olarak da değerlendirilebileceği görülmektedir. Örneğin ABD Federal Araştırma Bürosu (*Federal Bureau of Investigation*-FBI), ulus alt grupları veya gizli ajanlar tarafından bilgi, bilgisayar sistemleri, bilgisayar programları ve elektronik verilere yönelik yapılan planlı ve politik motivasyonlu saldırılar sonucu halk üzerinde şiddet ve panik oluşması durumunu "siber terörizm" olarak tanımlamaktadır.[32] Böylece, bilgisayar sistemlerine yönelik yapılan saldırılar sonucu, toplum nezdinde manevi hasar oluşması durumunda saldırganlar bilgisayar korsanı değil; terörist olarak adlandırılabilmekte ve eylemler için farklı tanımlamalar yapılabilmektedir. Örneğin, El Kaide bağlantılı internet aracılığıyla yapılan siber saldırılar için "elektronik cihat" tanımlamasının kullanıldığı[33] görülmektedir.

Sonuç olarak, uluslararası toplum (hatta devletler kendi içinde) hangi eylemin saldırı veya hangi eylemin saldırı tehdidi olduğu konusunda ittifak edememiştir. Bu durum, siber saldırı gibi kavramları tanımlamak, üzerinde uzlaşmak ve uluslararası barış ve güvenliği sağlamak konusunda gelecekte büyük zorluklarla karşı karşıya kalınacağını göstermektedir.[34] Bu bağlamda, gerçekleşen bir internet sitesi saldırısının faili; mağdur açısından "bilgisayar korsanı" iken, toplumun bir kısmı tarafından "bilgisayar korsanlığı eylemcisi" ve diğer bir kısmı tarafından "kahraman" olarak tanımlanabilmekte; devlet veya başka devletler açısından ise "terörist" olarak ilan edilebilmektedir.

[32] Aakashdeep Sharma ve Narinder Singh, "Cyber Terrorism And Cyber Laws: The Challenge For Governments", ***IAHRW International Journal of Social Sciences Review***, 2014, 2 (3), s. 1.
[33] Dorothy E. Denning, ***a.g.e.***, s. 176.
[34] Muharrem Gürkaynak ve Adem Ali İren, a.g.m., s. 276.

3.1. Bilgisayar Korsanlığı Kültüründe Sistem Kırıcılar

Bilgisayar korsanlığı kültüründe bilgisayar korsanı sadece sistem açıklıklarını kullanarak saldırıda bulunan kişi değil; aynı zamanda sosyal mühendislik olarak tanımlanan yöntemleri kullanan ve verdiği mesajlarla bir anda büyük yankı uyandırmayı becerebilen zeki insanlardır.

İnternetten ulaşılabilen, sistem açıklıklarının ve bu açıklıklardan nasıl istifade edilebileceğinin adım adım anlatıldığı dokümanları uygulayarak veya başkalarının bu amaçla ürettiği programları kullanarak sistemlere girmek "bilgisayar korsanlığı" değildir.[35] Bedava yazılımla insanların sistemlerine kişisel çıkar elde etmek için giren kişiler de "bilgisayar korsanı" olarak değil, "sistem kırıcı" olarak tanımlanmalıdır.[36] Google, Bing gibi arama motorları kullanılarak internet sitelerinde bulunan potansiyel açıklıkların basitçe öğrenilmesi ile "*Google Hacking*" olarak adlandırılan saldırı yöntemleri[37] sistem kırıcılar tarafından tercih edilmektedir. Hazır komut dizileri ve başkaları tarafından yazılan programlar kullanılarak sanal saldırıda bulunulması; gerçek bilgisayar korsanları tarafından küçümsenmekte ve "bilgisayar korsanlığı" olarak değil "yaramazlık" olarak[38] tanımlanmaktadır.

Sistem kırıcı ile bilgisayar korsanı arasındaki en önemli fark, sistem kırıcı açıklık zafiyeti bulduğu herhangi bir internet sitesine saldırı düzenleyip tahrif ederek mesaj bırakırken; bilgisayar korsanı ise, hedef olarak belirlediği internet sitesinde açıklık aramakta, sosyal mühendislik gibi farklı yöntemlerle "o internet sitesine" erişim sağlamakta ve mesaj bırakmaktadır.

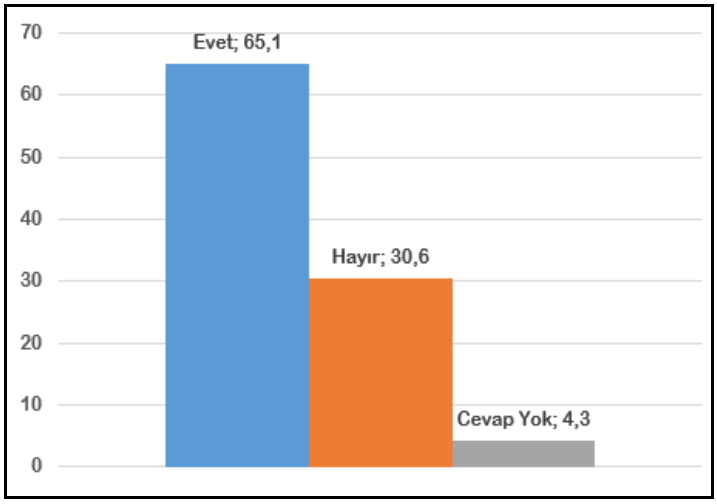
---

[35] Hakan Hekim ve Oğuzhan Başıbüyük, "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", ***Uluslararası Güvenlik ve Terörizm Dergisi***, 2013, 4 (2), 135-158, s. 142.
[36] Özgür Uçkan, 2013B, a.g.m., s. 46.
[37] HP İnternet Sitesi, Analysis of an Automated Mass Hack and Defacement Exploiting CVE-2013-5576, http://community.hpe.com/t5/Security-Research/HP-Security-Research - Threat-Intelligence-Briefing-Episode-8/ba-p/6248499, (Erişim Tarihi:01.12.2015), s. 5.
[38] Steven M. Furnell, The Problem of Categorising Cybercrime and Cybercriminals, ***2nd Australian Information Warfare and Security Conference***, 29-30 November 2001, Perth, Western Australia, 2011, p. 6.

3.2. Bilgisayar Korsanlığı Kültüründe Gizlilik

Bilgisayar korsanlarının tamamına yakınının takma isim kullanması ve deşifre olmamak için çeşitli yöntemler geliştirmesi, bilgisayar korsanlığı kültüründe gizliliğe verilen önemi göstermektedir. Örneğin ülkemizde bir dönem adından çokça söz ettiren RedHack'in verdiği röportajlarda, grup üyelerinin birbirlerini tanımadığını, memleket veya cinsiyet bilgilerinin bile bilinmediğini ifade etmesi, gizliliğe verilen önemi göstermektedir.

2009 yılında ülkemizde yapılan bir doktora çalışmasında, bilgisayar korsanları odaklı sitelere üye Türk bilgisayar korsanlarıyla anket yolu ile internet sitesi saldırısının suç olup olmadığının sorulması ve katılımcıların %65,1'inin "Evet" cevabını vermesi,[39] bilgisayar korsanlığı kültüründe gizliliğin nedeni hakkında ipucu vermektedir. Buna ilişkin sonuçlar Şekil 1'de yer almaktadır.



Şekil 1: İnternet Sitelerine Yönelik Bilgisayar Korsanlığı Suç Mudur?[40]

[39] Ufuk Eriş, ***a.g.e.***, s. 174.
[40] Ufuk Eriş, **a.g.e.**, s. 174.

Uluslararası bilgi güvenliği standartlarına göre, internet sitesi saldırıları "bütünlük ihlali"; site üzerinde yer alan verilerin ele geçirilmesi ve/veya yayınlanması ise "gizlilik ihlali" olarak sınıflandırılmaktadır.[41] Bu sınıflandırmaya paralel şekilde, ülkemiz ceza kanunlarında da düzenlemeler mevcuttur. TCK'nın 243'üncü maddesinin birinci fıkrasında, "bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girme ve orada kalmaya devam etme" suçu düzenlenmiştir. Aynı maddenin üçüncü fıkrasında ise "bu saldırı nedeniyle sistemin içerdiği verilerin yok olması veya değişmesi" durumunda cezanın arttırılması öngörülmüştür. Bir internet sitesinin yönetim paneline yetkisiz şekilde ulaşma, ücretli veya ücretsiz üyelik gerektiren bir alana üyelik hakkı olmaksızın girme ve benzeri eylemler bu madde kapsamına girmektedir. TCK'nın 244'üncü maddesinin birinci fıkrasında "bir bilişim sisteminin işleyişini engelleme veya bozma" ve ikinci fıkrasında "bilişim sistemindeki verileri bozma, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme" eylemleri düzenlenmiştir. 243'üncü maddeye göre daha ağır cezaî müeyyide içeren 244'üncü maddedeki tanımlamalar internet sitelerine yapılan DOS/DDOS saldırıları (erişilebilirlik ihlali) ve site sayfalarına mesajlar bırakılarak değişiklik yapılması eylemlerine (bütünlük ihlali) karşılık gelmektedir. Saldırı yapılan internet sitesinde kişilere ait kayıtlar, yazışmalar, fotoğraflar gibi özel hayatına ilişkin verilerin elde edilmesi (gizlilik ihlali) durumu, TCK'nın 134'üncü maddesinde "özel hayatın gizliliğini ihlal" suçu olarak düzenlenmiştir. Burada dikkat edilmesi gereken husus ise; verinin elde edilmesi suçun oluşması için yeterli olduğu ve üçüncü kişiler nezdinde ifşa edilmesi halinde cezada artırıma gidileceğidir.

Bilişim sistemlerine yönelik sistemi engelleme ve bozma eylemlerinde, kanun koyucu herhangi bir saike yer vermediğinden, suçun oluşması bakımından saik aranmayacaktır. Yine, aynı şekilde çalışmaması veya hatalı çalışması halinde doğabilecek hasardan çok sayıda insanın

[41] Hafize Keser ve Can Güldüren, a.g.m., s. 1168.

etkileneceği bir sisteme yapılan bir saldırıyla küçük bir şirketin internet sayfasına düzenlenen saldırı arasında da bir fark gözetilmemiştir.[42]

Her ne kadar bilgisayar korsanının sisteme sızarak yapmış olduğu illegal davranışların, devlet adına yapıldığında legal olarak görüldüğü[43] iddia edilse de, ülkemiz açısından TCK'da bu yönde bir düzenleme bulunmamaktadır. Bu bağlamda, toplumsal duyarlılık oluşturma, dünyanın başka bir bölgesinde meydana gelen haksızlığa dikkat çekme, maddi çıkar sağlama, kişisel olarak kendini ispatlama gibi hangi amaçla olursa olsun, bir bilişim sistemine yetkisiz olarak girme, bütünlüğüne zarar verme ve sistemde bulunan verileri ele geçirme suçtur ve kanuni yaptırımı bulunmaktadır. İşte bu gerçek, bilgisayar korsanlarını gizliliğe yönlendirmekte ve kimliklerini saklama zorunluluğu hissetmelerine neden olmaktadır.

3.3. Bilgisayar Korsanlığı Kültüründe Aleniyet

Bilgisayar korsanlığı ve övünmek iç içe geçmiştir. Her ne kadar politik bilgisayar korsanlığı eylemlerinde daha az düzeyde de olsa, övünmek ve başarı duygusu bilgisayar korsanlığı kültürünün ruhunda vardır.[44] Bu sebeple ister politik, ister maddi kazanç, isterse de kişisel tatmin amaçlı olsun, eylemi gerçekleştiren bilgisayar korsanı eyleminin geniş bir kitle tarafından duyulmasını ve kendisinin de takma isimle dahi olsa anılmasını istemektedir. Yapılan saldırılarda gizli bilgi temin etme ve istihbarat toplama gibi örtülü bir amaç yok ise, eylemin alenileştirilmesi amacıyla tahrif edilen internet sitelerine mesajlar bırakılmakta; eylem hakkında forum siteleri, sosyal medya ve farklı ortamlarda duyurular yapılmaktadır.

Tahrif edilen internet sitelerinin en büyük ortak özelliği, bilgisayar korsanları tarafından ziyaretçiler için mesajlar bırakılmasıdır.[45] Politik

[42] Hakan Hekim ve Oğuzhan Başıbüyük, a.g.m., s. 150.
[43] Mahruze Kara, ***a.g.e.***, s. 11.
[44] Özgür Uçkan, "Dijital Aktivizmin Sınır Boyunda Hacktivizm: Anonymous ve RedHack Örnekleri", (Der: Keleş, A.R. ve Sal, Y.), ***Hack Kültürü ve Hacktivizm: Yeni bir Siyaset Biçimi***, Alternatif Bilişim Derneği Yayını: İstanbul, 2013A, 53-79, s. 69.
[45] Kevin Borgolte et. al., ***a.g.e.***, p. 595.

olmayan site saldırılarında yayınlanan mesajlar; "bu sayfa hax0r tarafından ele geçirilmiştir!" gibi basit bir yazı, diğer bilgisayar korsanı arkadaşlarına "teşekkür" veya fotoğraf yayınlanması şeklindedir. Bilgisayar korsanlığı eylemciliğine dayalı saldırılarda ise politik mesajlar bırakılmaktadır. Bu mesajlar, saldırı yapılan organizasyonun eleştirilmesi olabileceği gibi, ilişkili başka organizasyona (hedef ülkeye ait herhangi bir internet sitesi) ait eleştiriler de olabilmektedir.[46]

Bilgisayar korsanları tarafından gerçekleştirilen eylemlerinin topluma duyurulması, başarılarının arşivlenmesi ve bununla övünülmesi amacıyla Zone-H internet sitesine kayıt yapılmaktadır.[47] Benzer amaçla, 1995-2001 yılları arasında yayın yapan Attrition (www.attrition.org), Nisan 2001 itibariyle artan saldırı kaydı taleplerini karşılayamama gerekçesi ile yeni kayıt almayı engellemiştir.[48] Bütünlük ihlali yapılan internet sitelerine ait ekran görüntülerinin kaydedildiği Zone-H (www.zone-h.org) internet sitesi ise 2002 yılında kurulmuştur. 01.01.2016 tarihi itibariyle sitede, 116.266 kayıtlı kullanıcı ve 11.270.816 internet sitesi saldırı kaydı mevcuttur. Siteye yapılan kayıtlar; kamu sitesi, ana sayfa saldırısı, aynı siteye daha önce yapılan saldırılar, aynı IP üzerinde toplu saldırılar ve bilgisayar korsanı tarafından yapılmış diğer saldırılar detaylı şekilde sınıflandırılmakta ve bu kayıtlarda sorgu yapılmasına imkân tanınmaktadır. Sitede, ayrıca, üyelere yönelik belirledikleri internet sitelerine saldırı olması durumunda haber vermek üzere erken uyarı sistemi mevcuttur. 01.01.2016 tarihi itibariyle 6064 kullanıcının Zone-H internet sitesi erken uyarı sistemine üyeliği bulunmaktadır.

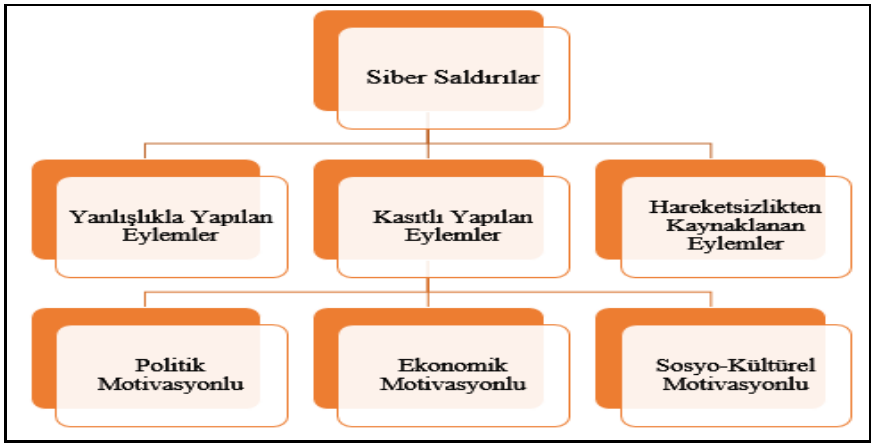
3.4. Bilgisayar Korsanlığı Kültüründe Motivasyon

Siber saldırılar, kişisel menfaat veya internet mafyasına hizmet etmek için yapılabilmektedir. Bilgisayar korsanlığı eylemciliğine dayalı gruplar ise saldırılarını siyasi hedeflerine propaganda yapmak, gürültü

[46] Alexandra Whitney Samuel, ***a.g.e.***, p. 56.
[47] HP İnternet Sitesi, Analysis of an Automated Mass Hack and Defacement Exploiting CVE-2013-5576, http://community.hpe.com/t5/Security-Research/HP-Security-Research-Threat-Intelligence-Briefing-Episode-8/ba-p/6248499, (Erişim Tarihi:01.12.2015), s. 32.
[48] Alexandra Whitney Samuel, ***a.g.e.***, p. 8.

çıkarmak ve dikkatleri üzerlerine çekmek için yapmaktadır. Devlet destekli saldırılar genellikle inkâr edilse de, hedef ülkenin siber ortamına müdahale etmek, ekonomik zarar vermek ve istihbarı bilgilerini ele geçirmek amaçlanmaktadır.[49] Siber saldırılarda motivasyon unsurunun anlaşılması için bilişim sistemlerine yönelik siber güvenlik risklerinin incelenmesi faydalıdır.

Siber güvenlik riskleri; yanlışlıkla yapılan eylemler, kasıtlı yapılan eylemler ve hareketsizlikten kaynaklanan eylemler olmak üzere üç sebepten kaynaklanmaktadır. Kasıtlı yapılan eylemler üç kategoriye ayrılmaktadır. Bunlar; hedefi yıkmak, bozmak ve kontrol altına almak, espiyonaj ve politik mesaj vermek amaçlı yapılan "politik motivasyonlu", hırsızlık, fikri mülkiyet ve sanayi casusluğu gibi maddi çıkar amaçlı yapılan "ekonomik motivasyonlu" ve politik, teolojik, felsefi, toplum yararına veya ego, merak ve ego amaçlı yapılan "sosyo-kültürel motivasyonlu" saldırılardır.[50] Siber saldırı motivasyonlarına ait özet bilgi Şekil 2'de yer almaktadır.



Şekil 2: Siber Saldırı Eylemleri ve Motivasyonları[51]

[49] Mahruze Kara, ***a.g.e.***, s. 5.
[50] Chen Han and Rituja Dongre, (2014), "What Motivates Cyber-Attackers?", ***Technology Innovation Management Review***, 2014, (Oct.2014), 40-42, p. 41.
[51] Chen Han and Rituja Dongre, a.g.m., p. 42.

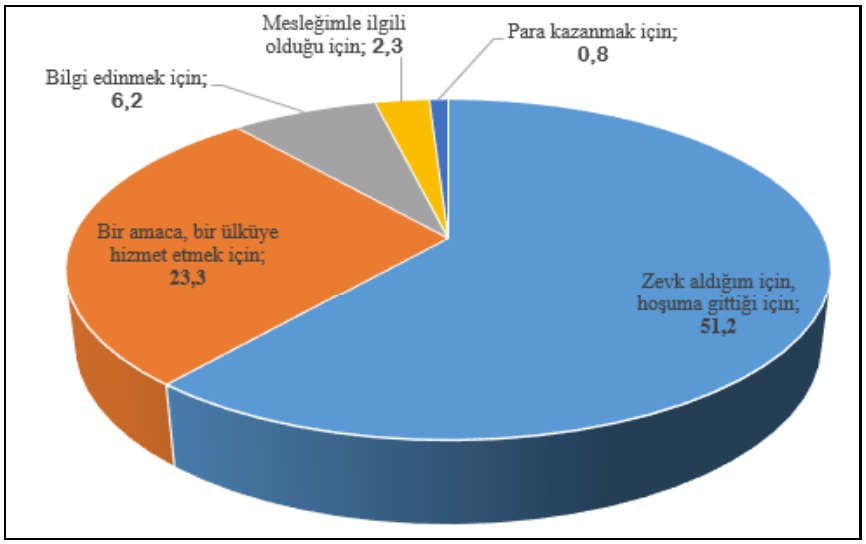
Furnell, siber saldırı yapan saldırganların bilgi seviyeleri ve dünya görüşlerinin farklı olduğunu vurguladıktan sonra, bilgisayar korsanlarının sınıflandırılması ile motivasyonları arasındaki farkın daha rahat görülebileceğini iddia etmektedir.[52] Furnell tarafından yapılan sınıflandırma Şekil 3'te yer almaktadır.

	Siber Terörist	Siber Saldırgan	Haktivist	Zararlı Kod Yazarı	Cracker
Meydan Okuma				✓	✓
Ego				✓	✓
Espiyonaj		✓		✓	
İdeoloji	✓	✓	✓		
Eğlence				✓	✓
Para		✓		✓	✓
İntikam	✓		✓	✓	

Şekil 3: Bilgisayar Korsanları ve Motivasyonları[53]

2009 yılında ülkemizde yapılan bir doktora çalışmasında, Türkiye'de bilgisayar korsanları alt kültürünün var olan durumunu değerlendirmek amacıyla, bilgisayar korsanları odaklı sitelere üye olan Türk bilgisayar korsanlarının 258'ine çevrimiçi anket uygulanmış ve 18 Türk bilgisayar korsanı ile mesajlaşma, yüz yüze veya telefonla olmak üzere görüşme yapılmıştır. Elde edilen verilere göre, internet sitesine yönelik bilgisayar korsanlığı gerçekleştirme nedenleri (motivasyonları) sırasıyla; "zevk alma, hoşa gitme", "bir amaca, ülküye hizmet etme", "bilgi edinme", "mesleki" ve "para kazanma" şeklinde olduğu görülmüştür.[54] Buna ilişkin sonuçlar Şekil 4'te yer almaktadır.

[52] Steven M. Furnell, ***a.g.e.***, p. 6.
[53] Steven M. Furnell, ***a.g.e.***, p. 7.
[54] Ufuk Eriş, ***a.g.e.***, s. 164.



Şekil 4: İnternet Sitelerine Yönelik Bilgisayar Korsanlığı Nedenleri[55]

Siber saldırı motivasyonu konusunda bahsedilmesi gereken önemli bir husus, belirli bir düşünceye hizmet etmekten ziyade, sistem açıklıklarından faydalanarak maddi kazanç elde etmek için yapılan siber saldırılardır. Maddi kazanç elde etmek amacıyla yapılan saldırılardan elde edilen verilerin kullanılması veya satılmasıyla "internet mafyacılığı" kavramı ortaya çıkmıştır.[56] Bilgisayar korsanları tarafından ele geçirilen kredi kartı bilgilerinin satıldığı, rakip şirketler için bilgisayar korsanlarının kiralandığı, kişisel verilerin el değiştirdiği, sistem açıklıklarının pazarlandığı bir sektör ortaya çıkmıştır ki, bu durum "Bilgisayar Korsanı Pazarı" olarak da adlandırılmaktadır.[57] Bu sektörün öncülerinden *CarderPlanet* ve *DarkMarket* isimli forum sitelerine yapılan operasyonlar dünya genelinde büyük yankı uyandırmıştır. Çok sayıda ülkenin koordinasyonlu çalışması sonucu yapılan operasyonla, ABD ve Türkiye'nin de aralarında

[55] Ufuk Eriş, ***a.g.e.***, s. 164.
[56] Mahruze Kara, ***a.g.e.***, s. 25.
[57] Lillian Ablon et. al., "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar", ***USA National Security Research Division***, 2014, p .4.

bulunduğu birçok ülkede çok sayıda siber suçlu yakalanmıştır.[58] Bununla birlikte, sanal ortamda bu tür faaliyetlerin devam ettiği ve yetkisiz şekilde ele geçirilen bilginin maddi kazanç konusu yapıldığı platformların bulunduğu iddia edilmektedir.

4. Türkiye'de Kamuya Ait İnternet Sitelerine Yapılan Siber Saldırılar

Bilgisayar korsanları tarafından siber saldırı düzenlenebilecek kamu kuruluşları, özel şirketler, polis ve sağlık sektörü tarafından kullanılan çağrı merkezleri gibi çok sayıda hedef bulunması; saldırı düzenlenebilecek zayıf halka bulunmasını kolaylaştırmaktadır.[59] Teknolojik anlamda güçlü olan devletlerin, bilişim sistemlerine bağımlılıkları sebebiyle saldırıya en açık devlet olmaları[60] ve daha fazla saldırıya uğramaları normaldir.

Denning'e göre, siber saldırılar bilgisayar korsanlığı eylemleri, elektronik cihat ve vatansever saldırılar olmak üzere üçe ayrılmaktadır. Siber saldırıların sosyal ve politik aktivizmin amaçlı yapıldığı bilgisayar korsanlığı eylemlerinde de hedef kamu kurumları, ulusal ve uluslararası şirketlerdir. El Kaide'nin terörist faaliyetlerine destek vermek amaçlı yapılan siber saldırılarda hedef başta ABD ve diğer Batı ülkeleri olmak üzere devlet kurumları ve hükümet dışı kuruluşlardır. Vatansever saldırılar devlet-devlet çatışması olmakla birlikte, failler hükümetler değil; vatandaşlar ve gurbetçilerdir. Vatansever saldırılarda hedef, karşı devlete ait kamu ve hükümet dışı kuruluşlardır.[61] Bu bağlamda bilgisayar korsanlarının motivasyonu farklı olsa da, ortak saldırı hedefleri büyük oranda kamu kurumlarına ait internet siteleri olduğu anlaşılmaktadır.

İnternetin iz sürülebilme konusunda güçlükler içeren doğası gereği, siber saldırıların kaynağı net olarak tespit edilememektedir.[62] ABD'de 2004 yılında yapılan bir doktora çalışmasında; Kasım 2000 ayında ortaya

[58] Jonathan Lusthaus, "Electronic Ghosts", ***Democracy Journal***, 2014, 31, 45-57, p. 51.
[59] Muharrem Gürkaynak ve Adem Ali İren, a.g.m., s. 267.
[60] Şeyda Türkay, "Siber Savaş Hukuku Ve Uygulanma Sorunsalı", ***İstanbul Üniversitesi Hukuk Fakültesi Mecmuası***, 2013, 71 (1), 1177-1228, s. 1217.
[61] Dorothy E. Denning, ***a.g.e.***, s. 172.
[62] Mehmet Nesip Öğün ve Adem Kaya, a.g.m., s. 164.

çıkan ve iki yıl boyunca Hindistan ve İsrail karşıtı çok sayıda siber saldırı düzenleyen WFD (*World's Fantabulous Defacers*) bilgisayar korsanı grubu ele alınmış ve grup hakkında detaylı bilgi, saldırı yapılan sitelere bırakılan mesajlar ve Zone-H kayıtlarından temin edilmiştir.[63] 2010 yılında Pakistanlı "*Pak Cyber Army*" ve "*PakHaxors*" isimli bilgisayar korsanları grupları ile Hindistanlı "*Indishell*" ve "*Indian Cyber Army*" isimli bilgisayar korsanları grupları arasında karşılıklı yapılan siber saldırıların ele alınmasında da Zone-H kayıtlarına atıfta bulunulmuştur.[64] Bu sebeple, çalışmada internet sitesi saldırıları değerlendirilirken, Zone-H kayıtları temel veri kaynağı olarak tercih edilmiştir.

BTK tarafından yayınlanan Üç Aylık Pazar Verileri Raporuna göre; 2015 yılı ikinci çeyrek itibarıyla "nic.tr" kayıtlarında 367.342 adet ".tr" uzantılı alan adı bulunmaktadır. Bu alan adlarının %76,8'i "com.tr", %6,8'i "gen.tr", %3,6'sı "gov.tr", %3,0'ı ise "web.tr" uzantısına sahiptir.[65] Yayınlanan verilere göre, ülkemizde 13.224 ".gov.tr" uzantılı internet sitesi bulunmaktadır. Zone-H kayıtlarına göre, 2002 yılından 2015 yıl sonuna kadar ülkemizde kamuya ait ".gov.tr" uzantılı internet sitelerine yönelik gerçekleştirilen saldırı sayısı 8.998 olup bu saldırıların 3.602'si tekil, 5.396'sı ise toplu saldırı şeklindedir. 8.998 saldırı içerisinde aynı internet sitesine ait mükerrer saldırılar, aynı internet sitesinin farklı sayfalarına ait saldırılar ve aynı internet sitesine ait farklı alt etki alanı saldırıları olmakla beraber 8.998 saldırı sayısının oldukça yüksek olduğu açıktır.

Bu çalışmada Zone-H internet sitesinde yer alan kayıtlardan 2015 yılına ait ".gov.tr" uzantılı internet sitelerine yönelik gerçekleştirilen 848 saldırı kaydı ele alınmıştır. Bu saldırılar aylara göre saldırı bilgileri, ana sayfa saldırı bilgileri, geçmiş saldırı bilgileri, sunuculara ait bilgiler ve saldırganlara ait bilgiler olmak üzere beş açıdan analiz

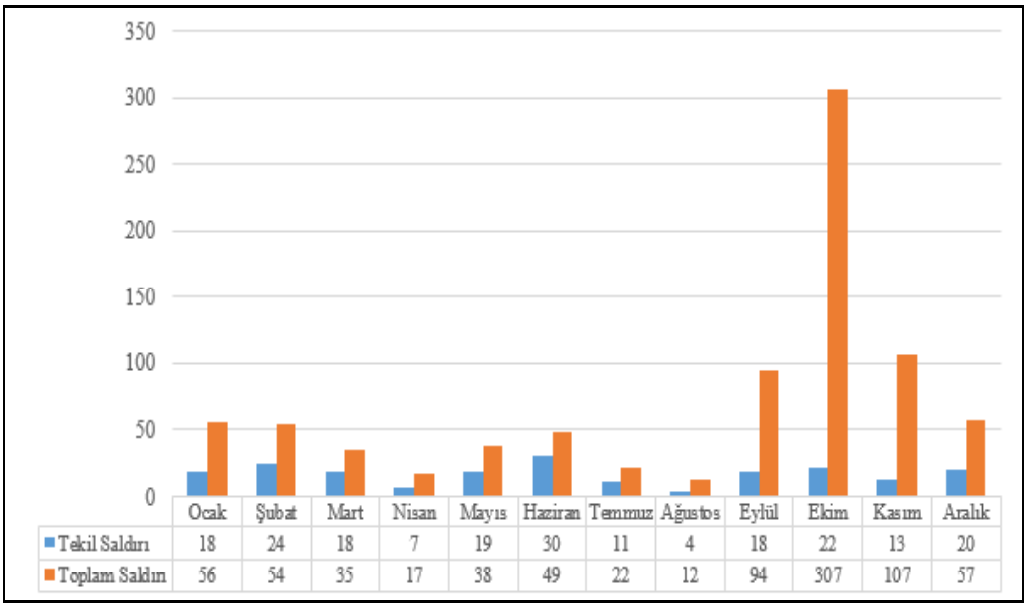
[63] Alexandra Whitney Samuel, a.g.e., p. 56.
[64] Vaidehi Sachin, ***Cyber Terror – The Hidden Crime***, Quality Printers: Hindistan, 2010, s. 64.
[65] ***BTK Üç Aylık Pazar Verileri Raporu: 2015 Yılı 2. Çeyrek***, Bilgi Teknolojileri ve İletişim Kurumu, Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı, Ankara, 2015, s. 10.

edilmiştir. Çalışmaya konu verilerin sadece Zone-H kayıtlarına dayanması ve çalışmada sadece ".gov.tr" uzantılı kamu sitelerinin dikkate alınması ve ".edu.tr" gibi farklı uzantılı kamu internet sitelerinin çalışmaya dâhil edilmemesi ise çalışmanın en büyük sınırlılığı olmuştur. Zone-H'da 2015 yılına ait ".mil.tr" ve ".pol.tr" uzantılı internet siteleri ile ilgili herhangi bir kayıt bulunmadığı anlaşılmıştır.

4.1. Aylara Göre Saldırı Bilgileri

İnternet sitelerine yapılan saldırılar Zone-H kayıtlarında "tekil saldırı" (*single IP*) ve "toplu saldırı" (*mass defacement*) olarak kategorize edilmektedir. Bilgisayar korsanları tarafından sunucu üzerinde bulunan bir açıklıkla sunucu üzerinde bulunan tüm internet sitelerine toplu olarak saldırı yapılması "toplu saldırı" olarak tanımlanmaktadır. Zone-H kayıtlarına göre, 2015 yılında gerçekleşen 848 saldırının 204'ünün tekil saldırı, 644'ünün ise toplu saldırı olduğu görülmektedir. Buna göre, tekil saldırı sayısının toplam saldırı sayısına oranının yaklaşık 1/4 seviyesinde olduğu görülmektedir. Böylece bilgisayar korsanlığına maruz kalan internet sitelerinin büyük kısmının aynı IP adresinde yayın yaptığı anlaşılmaktadır.

Ülkemizde kamu kurumlarına ait internet sitelerine yapılan tekil saldırılar aylara göre incelendiğinde, Temmuz ve Ağustos aylarında nispeten azalma olmakla beraber, yıl boyunca her ay ortalama 18 internet sitesine saldırı düzenlendiği anlaşılmaktadır. Buna ilişkin veriler Şekil 5'te yer almaktadır.



Şekil 5: 2015 Yılında Saldırıya Uğrayan Kamu Sitelerinin Aylara Göre Dağılımı[66]

Küçük ve orta ölçekli internet sitelerine yönelik yapılan tekil saldırılar çoğu zaman önemsiz görülmekle birlikte, günlük binlerce internet sitesinin saldırıya uğraması, önemli gider ve verimlilik kaybına neden olmaktadır. Bu saldırıların birçoğunda ise toplu saldırı araçları kullanılmakta, hızlı bir şekilde internet sitelerinde var olan açıklıklar tespit edilmekte ve "*0day exploit*"e dönüştürülmektedir.[67] Toplu saldırılar aynı IP üzerinde yayın yapan birden fazla internet sitesinin tek seferde tahrif edilmesi ve bütünlük ihlalinin yaşanması anlamına gelmektedir. Bu durumun sebebi, aynı kuruma ait farklı hizmet, birim ve şubelere

[66] Bu tablo Zone-H internet sitesinde yer alan "Special Defacement" verilerinden elde edilerek oluşturulmuştur. http://www.zone-h.org/archive/special=1, (Erişim Tarihleri: 10.11.2015 ve 01.01.2016).

[67] HP İnternet Sitesi, Analysis of an Automated Mass Hack and Defacement Exploiting CVE-2013-5576, http://community.hpe.com/t5/Security-Research/HP-Security-Research-Threat-Intelligence-Briefing-Episode-8/ba-p/6248499, (Erişim Tarihi: 01.12.2015), s. 3.

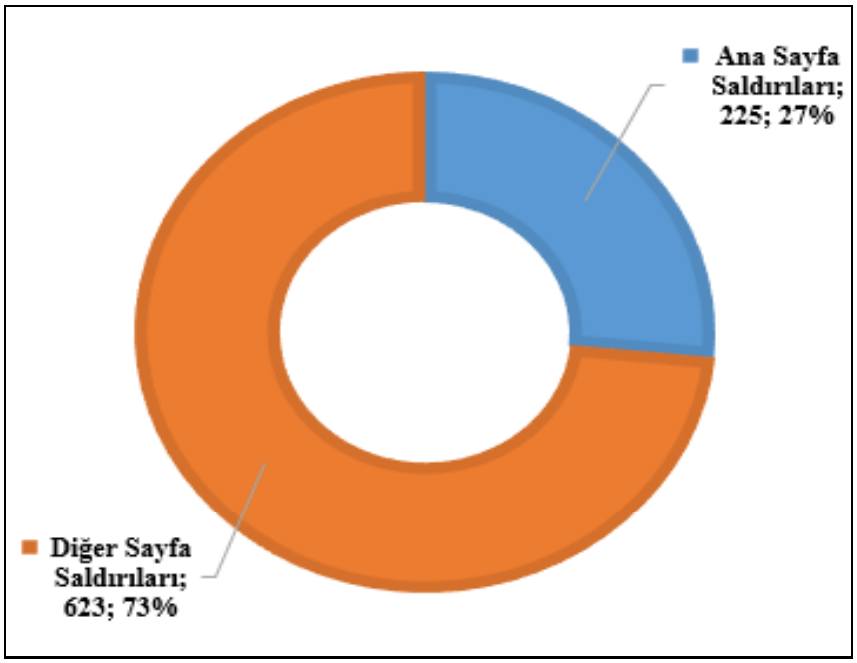
ait internet sitelerinin aynı IP adresi üzerinde ve (büyük çoğunluğunun) aynı etki alanı üzerinde farklı alt etki alanları yayın yapmasıdır. Örneğin, ülkemizde A kurumuna ait www.akurumu.gov.tr internet sitesinde bulunan bir zafiyet doğrudan kurumun 81 il yapılanmasına ait internet sitelerini (www.istanbul.akurumu.gov.tr gibi) de tehdit etmektedir.

Aylara göre saldırılarda, Temmuz ve Ağustos aylarında göreceli bir azalma olması; saldırıların yaz aylarında azaldığı izlenimini oluşturmakla beraber, bu konuda net bir değerlendirme yapabilmek için aynı döneme ait geçmiş yıllara ait kayıtların da incelenmesi, yakalanan bilgisayar korsanlarının yaş-eğitim durumlarının değerlendirilmesi ve bu yönde bir ifadelerinin bulunup bulunmadığının araştırılması gerekmektedir. Yapılan literatür taramasında bu çerçevede bir tespitte bulunulamamıştır.

Tekil ve toplu saldırı arasındaki ciddi fark bulma nedeni örnek verilerek açıklanmıştır. Birçok kurumda, internet sitesi güvenliğinin merkez teşkilatı bilgi işlem birimleri tarafından sağlandığı ve taşra birimlerince sadece veri girişi yapıldığı dikkat alındığında, merkez birimlerince alınan/alınacak güvenlik tedbirlerinin önemi ortaya çıkmaktadır.

4.2. Ana Sayfa Saldırı Bilgileri

2015 yılında ülkemizde kamu kurumlarına ait internet sitelerine yönelik gerçekleştirilen 848 saldırı incelendiğinde bu saldırıların 255'inin internet sitesinin ana sayfasına yönelik olduğu görülmektedir. Buna ilişkin veriler Şekil 6'da yer almaktadır.



Şekil 6: 2015 Yılında Türk Kamu İnternet Sitelerine Yönelik Ana Sayfa Saldırısı Dağılımı[68]

Bir internet sitesinin ana sayfasına bırakılan mesajların kısa sürede daha fazla kullanıcı tarafından görülmesi sebebiyle, toplum üzerindeki kısa sürede daha fazla etki bırakmaktadır. İnternet sitelerinin alt dizininde bulunan bir sayfaya (örneğin www.akurumu.gov.tr/duyurular/güncelihaleler/sandalyeihalesi.php) yapılan saldırı ve bırakılan bir mesaj ise sınırlı sayıda kullanıcı tarafından fark edilebilmekte bazı durumlarda ise sadece sistem yöneticileri tarafından tespit edilebilmektedir. Bu açıdan bilgisayar korsanları tarafından ana sayfa saldırılarına daha fazla önem verilmekte ve ana sayfa saldırıları prestij olarak değerlendirilmektedir.

[68] Bu tablo Zone-H internet sitesinde yer alan "Special Defacement" verilerinden elde edilerek oluşturulmuştur. http://www.zone-h.org/archive/special=1, (Erişim Tarihleri: 10.11.2015 ve 01.01.2016).

4.3. Geçmiş Saldırı Bilgileri

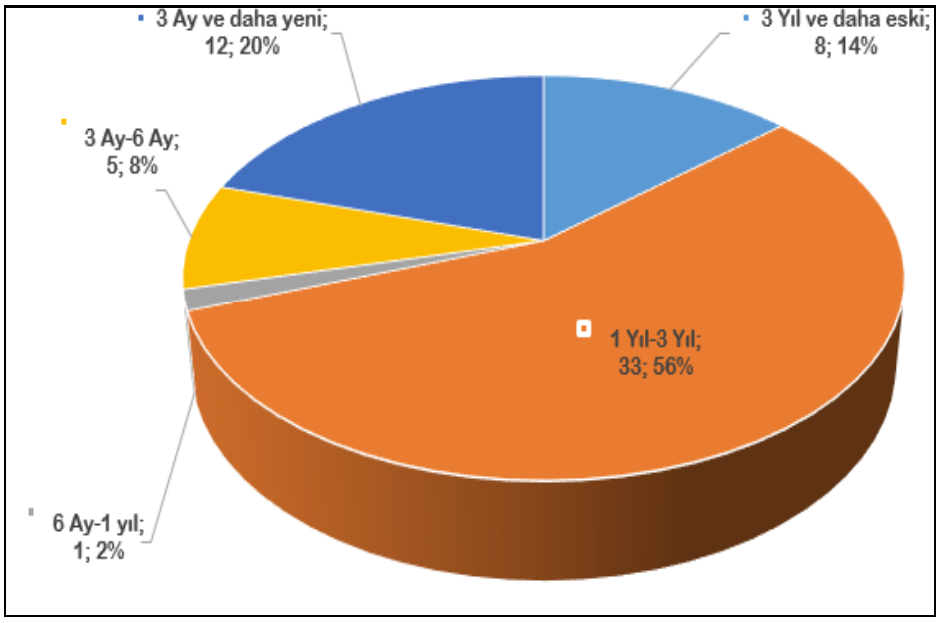
2015 yılında ülkemizde kamu kurumlarına ait 848 internet sitesine saldırı gerçekleşmekle beraber toplam 297 internet sitesinin geçmişte de saldırıya uğradığı anlaşılmaktadır. Geçmiş saldırılar analiz edildiğinde ise aynı internet sitesine tekrar yapılan saldırılarda, saldırganların büyük kısmının farklı olduğu görülmektedir. Böylece, bilgisayar korsanlarının saldırdıkları internet sitelerine tekrar saldırma konusunda özel bir çaba içerisinde olmadıkları sonucuna ulaşılması mümkündür.

Siber güvenlik olaylarıyla ilgili saldırı şekilleri ve bunlara karşı korunma tedbirlerinin kaydedildiği ve gerektiğinde ilgililerce erişilebilecek bir veri tabanı oluşturulması, benzer saldırılar meydana gelmesi durumunda iş gücü ve zaman kaybının azaltılmasını ve hatta ortadan kaldırılmasını sağlamak açısından son derece önemlidir.[69] Bu bağlamda, internet sitelerinin güvenliğinden sorumlu görevlilerin yaşanan saldırılar sonrası detaylı analiz yapılarak kullanılan yol ve yöntemlerin deşifre edilmesi, var olan açıklıkların kapatılması ve elde edilen bulguların ortak veri tabanlarına aktarılmasının fayda sağlayacağı açıktır.

2015 yılı Kasım ayında ülkemize ait saldırıya uğrayan 107 kamu internet sitesi incelendiğinde; 48 internet sitesinin ilk defa; 50'sinin iki defa; altısının üç defa; ikisinin dört defa ve birinin ise beş defa saldırıya uğradığı görülmektedir.

Daha önce saldırıya uğrayan 59 internet sitesinin geçmiş saldırıların 12'sinin üç ay içinde; beşinin üç ay içinde; birinin 6-12 ay içerisinde; 33'ünün bir ile üç yıl içinde 18'inin bir yıl içinde ve 38'inin bir yıldan daha az süre içinde gerçekleşmiş olduğu anlaşılmaktadır. 2015 yılı Kasım ayına ilişkin saldırıya uğrayan Türk kamu internet sitelerine ilişkin bilgiler Şekil 7'de yer almaktadır.

[69] Mehmet Nesip Öğün ve Adem Kaya, a.g.m., s. 174.

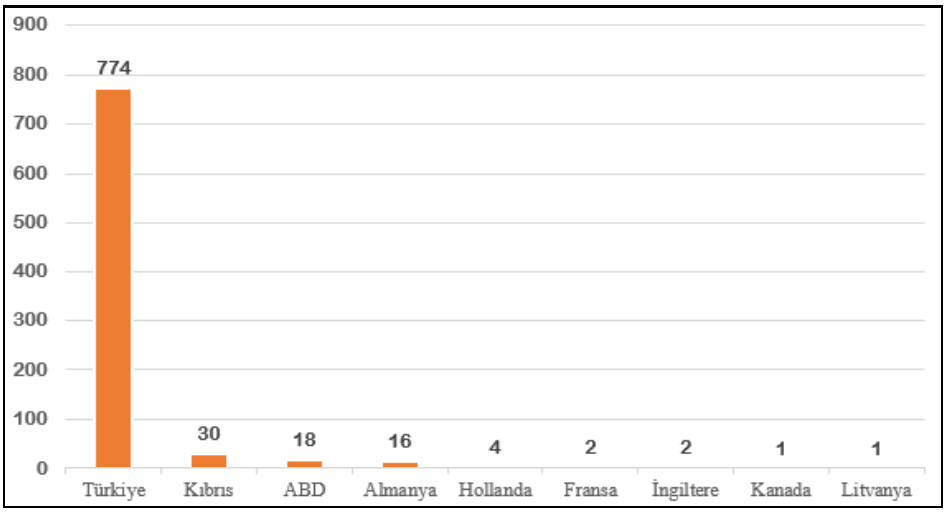


Şekil 7: 2015 Yılı Kasım Ayında 2'nci Defa Saldırıya Uğrayan Türk Kamu Siteleri[70]

4.4. Sunuculara Ait Bilgiler

2015 yılında ülkemizde kamu kurumlarına ait internet sitelerine yönelik gerçekleştirilen 848 saldırıya ait sunucu bilgileri incelendiğinde; saldırıya uğrayan internet sitelerinden 774'ünün Türkiye'de yayın yaptığı, diğerlerinin ise yurtdışında yayın yaptığı anlaşılmaktadır. 2015 yılında saldırıya uğrayan Türk kamu internet siteleri sunucularına ait yer bilgileri ülkelere göre Şekil 8'de yer almaktadır.

[70] Bu tablo Zone-H internet sitesinde yer alan "Special Defacement" verilerinden elde edilerek oluşturulmuştur. http://www.zone-h.org/archive/special=1, (Erişim Tarihleri: 10.11.2015 ve 01.01.2016).



Şekil 8: 2015 Yılında Saldırıya Uğrayan Kamu Siteleri Sunucularına Ait Yer Bilgileri[71]

Şirket içinden yapılan saldırılar önemli bir tehdittir. Sistem ile ilgili alınan güvenlik tedbirlerini en iyi içeride çalışanlar bilmekte ve art niyetli çalışanlar taşınabilir bellekler aracılığıyla özel bilgileri kolayca çalabilmektedir.[72] Şirket çalışanlarının maddi çıkar, tehdit veya başka bir sebeple sistem güvenlik açıklarını veya doğrudan sistemde bulunan verileri üçüncü kişilerle paylaşması mümkündür. Siyasi olarak problem yaşanan karşı devlete ait internet sitelerine yönelik millî ve manevi duygularla şirket çalışanları tarafından suistimalde bulunulması da ihtimal dâhilindedir.

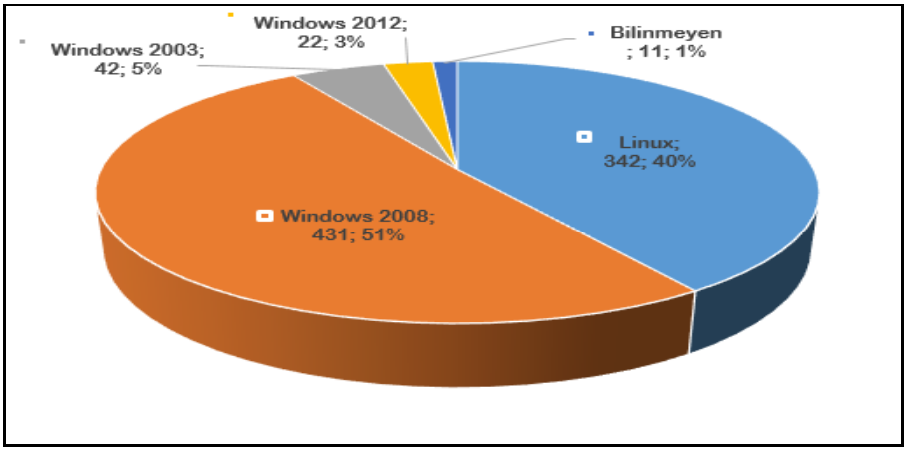
Özellikle ".gov.tr" uzantılı internet sitelerinin yurtdışında başka ülkelere ait sunucularda yayın yapmasının başlı başına bir risk oluşturduğu değerlendirilmektedir. Bu durum, kamu kurumları tarafından ekonomik

[71] Bu tablo Zone-H internet sitesinde yer alan "Special Defacement" verilerinden elde edilerek oluşturulmuştur. http://www.zone-h.org/archive/special=1, (Erişim Tarihleri: 10.11.2015 ve 01.01.2016).

[72] Okechukwu Wori, "Computer Crimes: Factors of Cybercriminal Activities", ***International Journal of Advanced Computer Science and Information Technology***, 2014, 3 (1), 51-67, p. 61.

sebeplerle yapılan bir tercih sonucu ortaya çıkmış olabileceği gibi; yer sağlayıcıları tarafından ve kurum yetkilisinin bu yönde rızası olmaksızın yurtdışında bulunan bir sunucudan alan sağlamış olmasıyla da mümkün olmaktadır. Siber savaş ve bilgi hırsızlığı gibi konuların tartışıldığı günümüzde bu durumun ülkemiz açısından zafiyet oluşturacağı açıktır.

Saldırıya uğrayan internet sitelerinin yayın yaptığı sunuculara ait işletim sistemi bilgileri incelendiğinde, 495 internet sitesinin Windows işletim sistemi üzerinde; 342 internet sitesinin ise Linux işletim sistemi üzerinde yayın yaptığı anlaşılmaktadır. İşletim sistemi bilgilerine ait bilgiler Şekil 9'da yer almaktadır.



Şekil 9: 2015 Yılında Saldırıya Uğrayan Kamu Siteleri Sunucularına Ait İşletim Sistemi Bilgileri[73]

Sistem yöneticileri tarafından internet sitesi yönetimi Dreamweaver veya KompoZer gibi web editörleri, FTP programları veya Secure Shell (SSH) programları ile yapılmaktadır. Bu sebeple, birçok sistem yöneticisi sunucuda bulunan işletim sistemi türüyle ilgilenmemektedir.

[73] Bu tablo Zone-H internet sitesinde yer alan "Special Defacement" verilerinden elde edilerek oluşturulmuştur. http://www.zone-h.org/archive/special=1, (Erişim Tarihleri: 10.11.2015 ve 01.01.2016).

Diğer taraftan ASP, .NET, MSSQL veya Access gibi Windows tabanlı teknolojilerin kullanılan internet sitelerinde genellikle kolaylık açısından Windows işletim sistemini tercih edilmektedir.[74] Windows işletim sistemlerinde bulunan ağ paylaşımlarında gerekli sınırlamalar yapılmaması, saldırganlarca kullanılan otomatik araçlarla suistimal edilebilmektedir.[75] İnternet sitesi saldırılarında sıklıkla kullanılan SQL girişlerine ve XSS saldırısına karşı kod açıklıklarına (eksik kod, hatalı kod, vb.) dikkat edilmeli; ayrıca kullanılan uygulamaların güncel olması sağlanmalıdır.[76] Bu bağlamda kullanılan bilgi teknolojileri ürünlerinde ve sistemlerinde siber güvenlik standartlarında test ve belgelendirme yapılmasıyla[77] kullanıcı kaynaklı hataların önüne geçilebilecektir.

Bilişim teknolojilerinde bulunan açıklıkların yayınlandığı Yaygın Güvenlik Açıkları ve Etkilenmeler (*Common Vulnerabilities and Exposures*-CVE) verilerine göre; Windows Server 2000'de 507, Windows Server 2003'de 855, Windows Server 2008'de 636 ve Windows Server 2012'de 249 açıklık bulunmaktadır.[78] Bu açıdan bakıldığında, internet sitesinin yayın yaptığı sunucu üzerinde hangi işletim sistemi ve türü olursa olsun güncellemelerin düzenli olarak yapılması ve yayınlanan açıklıkların takip edilmesi gerekmektedir. Ayrıca sunucudaki verilerin belirli periyotlarla düzenli bir şekilde yedeklerinin (*backup*) alınması, olası saldırı durumunda zararın en aza inmesini ve vatandaşlara sunulan hizmetlerin aksamamasını sağlayacaktır.

[74] Christopher Heng, "Should You Choose a Linux or a Windows Web Hosting Package? And Is There Such a Thing as a Mac Web Host?", http://www.thesitewizard.com/webhosting/linux-vs-windows.shtml, (Erişim Tarihi: 10.12.2015).

[75] Harkarandeep Kaur, et. al., "Analyzing Website Hacking Tool and Their Prevention Techniques", ***International Journal of Computer and Communication System Engineering***, 2015, 2 (3), 523-529, s. 525.

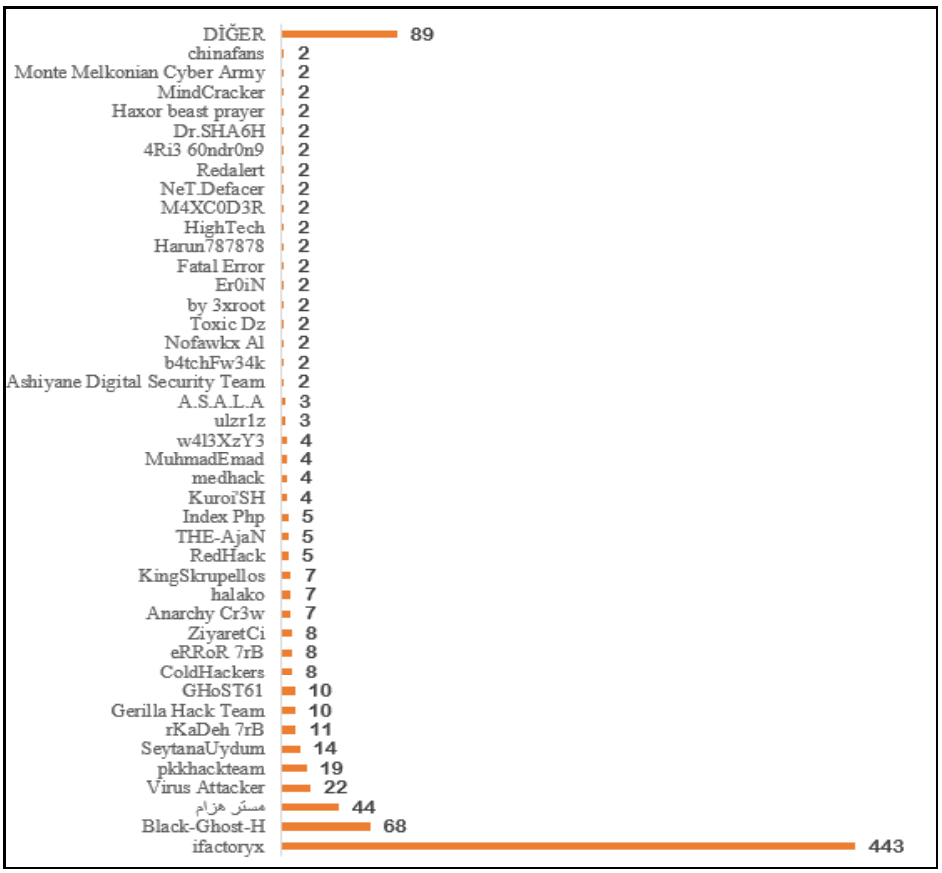
[76] Sandra Sarasan, a.g.m., s. 34.

[77] Mariye Umay Akkaya, Siber Güvenlik Standartları ve Belgelendirmeleri, ***ICSG İSTANBUL 2014-Uluslararası İstanbul Akıllı Şebekeler ve Şehirler Kongre ve Fuarı***, 8-9 Mayıs 2014, Bildiri Kitabı, İstanbul, 2014, ss. 48-52, s. 49.

[78] CVE Details İnternet Sitesi, Top 50 Products By Total Number Of "Distinct" Vulnerabilities, https://www.cvedetails.com/top-50-products.php, (Erişim Tarihi: 10.12.2015).

4.5. Saldırganlara Ait Bilgiler

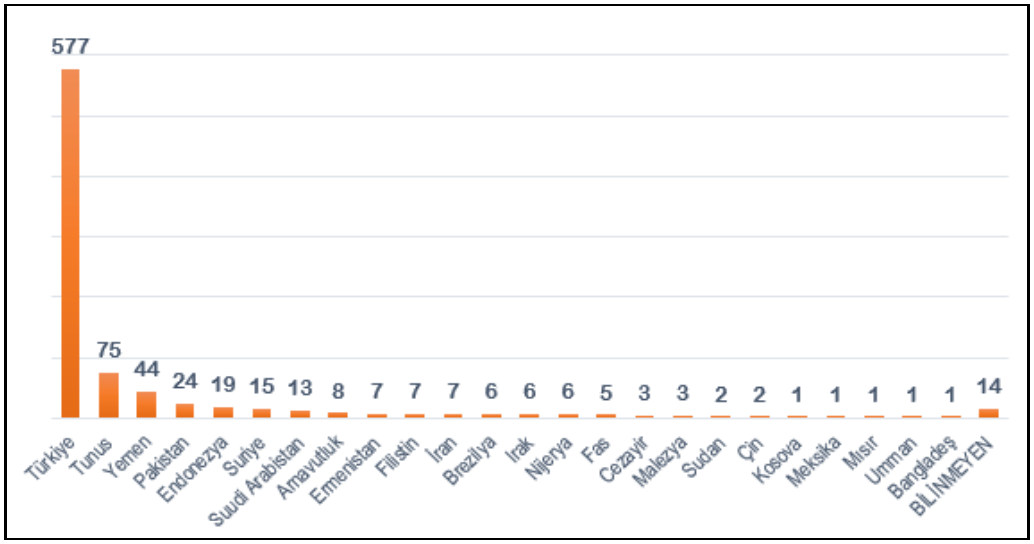
2015 yılında ülkemizdeki kamu kurumlarına ait internet sitelerine yönelik gerçekleştirilen 848 saldırı toplam 131 farklı saldırgan/grup tarafından gerçekleştirilmiştir. Zone-H kayıtlarında yer alan saldırgan isimleri ve saldırı sayıları Şekil 10'da yer almaktadır. Toplam 89 saldırgan tarafından gerçekleştirilen birer saldırı ise "diğer" olarak gösterilmiştir.



Şekil 10: 2015 Yılında Türk Kamu İnternet Sitelerine Saldırı Gerçekleştiren Saldırgan Bilgileri[79]

[79] Bu tablo Zone-H internet sitesinde yer alan "Special Defacement" verilerinden elde edilerek oluşturulmuştur. http://www.zone-h.org/archive/special=1, (Erişim Tarihleri:

Bilgisayar Korsanları ve Bilgisayar Korsanlığı Kültürü başlıklı bölümde, saldırganlar tarafından bir takma isim belirlendiği ve tahrif edilen (bütünlüğü bozulan) internet sitesine mesajlar bırakıldığından bahsedilmişti. Sadece tahrif edilen internet sitelerine bırakılan mesajlar ve saldırgana ait takma isimler ile bir şahıs/grup/ülkeyi sorumlu tutmak yeterli değildir. Bununla beraber, bırakılan mesajlar incelendiğinde Şekil 11'deki sonuçlar elde edilmiştir.



Şekil 11: 2015 Yılında Türk Kamu İnternet Sitelerine Yönelik Saldırı Gerçekleştirenlerin Ülke Bilgileri[80]

Saldırılara ait ülke bilgileri incelendiğinde, saldırıların %70'inin Türkiye merkezli olduğu ve toplamda 25 farklı ülkeden saldırı yapıldığı görülmektedir. Bununla beraber, saldırı mesajları incelendiğinde,

10.11.2015 ve 01.01.2016).

[80] Bu tablo Zone-H internet sitesinde yer alan "Special Defacement" verilerinde yer alan saldırıya uğramış (tahrif edilmiş) internet sitelerine bırakılan mesajlar (yazı, resim vb.) incelenerek oluşturulmuştur. http://www.zone-h.org/archive/special=1, (Erişim Tarihleri: 10.11.2015 ve 01.01.2016).

saldırıların bir kısmının Türkiye politikaları ve saldırıya uğrayan kamu kurumlarının uygulamaları ile ilgili olmadığı ve saldırının siyasi bir yönünün bulunmadığı anlaşılmaktadır. Bu bağlamda, yapılan saldırıların IP-tarama yöntemi ile rastgele seçilmiş olabileceği ve kişisel ego/tatmin amacıyla yapılmış olabileceği değerlendirilmektedir.

Tunus, Yemen ve Pakistan başta olmak üzere yapılan saldırıların büyük bir kısmında bırakılan mesajların "Filistin'e özgürlük", "Müslümanlar terörist değildir" vb. şekilde olduğu veya ABD ve İsrail karşıtı söylemler içerdiği görülmektedir. Brezilya ve Endonezya başta olmak üzere yapılan saldırıların bir kısmında ise müzik ve fotoğraf paylaşımı yapıldığı anlaşılmaktadır. Yurtdışından yapılan saldırıların sadece küçük bir kısmında Türkiye'nin Suriye politikasının eleştirildiği görülmektedir. Bu açıdan, Türkiye harici saldırıların ülkemiz açısından siyasi/politik yönünün bulunmadığı ve rastgele seçilmiş hedef saldırısı olduğu anlaşılmaktadır.

Ülkemizden yapılan saldırıların bir kısmında "açıklıklarınızı kapatın" şeklinde uyarı şeklinde mesajlar bırakıldığı veya ABD ve İsrail karşıtı söylemler içerdiği ve ülke politikaları ile ilgili içerik bulunmadığı anlaşılmaktadır. Diğer taraftan saldırıların bir kısmında "Kürtlere özgürlük", "Kürdistan Katliamlarına Dur Diyeceğiz", "Serbest bilgi akışı engellenemez" gibi siyasi/politik mesajlar bulunduğu ayrıca terör örgütü PKK/KCK lehine resim ve video paylaşımlarının bulunduğu görülmektedir.

5. Sonuç ve Değerlendirme

Bilgisayar kullanımı ve internet erişiminin yaygınlaşması, insanların alışkanlıklarında büyük değişiklikler yapmış ve yaşamın bir parçası haline gelmiştir. Devletler tarafından bilgilendirme amaçlı internet sitelerinin kurulması ve bir kısım kamu hizmetlerinin bu internet siteleri aracılığıyla gerçekleştirilmesi; günlük hayatta zaman, emek ve maddi tasarruf sağlamıştır.

Toplumlar üzerinde bunca olumlu faydası bulunan internet sitelerine yönelik çeşitli motivasyonlarla siber saldırılar düzenlenmekte ve bu siteler mesaj verme, meydan okuma ve kendini ispat etme ortamı haline getirilmektedir. Bu durum, ticari açıdan kazanç ve itibar kaybına neden olurken, kamu kurumları açısından toplum üzerinde negatif

algıların oluşmasına neden olabilmektedir. Kamuya ait internet sitelerinin siyasi kararlara ve politikalara tepki olarak yetkisiz bir şekilde mesaj yayınlama ortamı olarak kullanılması, kabul edilemeyecek bir durumdur. Bu açıdan kamu kurumlarına yapılan siber saldırıların analiz edilmesi, tekrarlanmamasına yönelik tedbirlerin alınması ve üzerinde akademik çalışmaların yapılması gerekmektedir.

Bu çalışmada, 2002 yılından itibaren internet sitelerine yapılan saldırıların bilgisayar korsanları tarafından kaydedildiği Zone-H (www.zone-h.org) kayıtları ele alınmıştır. Zone-H üzerinde 2015 yılına ait ".gov.tr" uzantılı toplam 848 saldırı kaydı; ana sayfa saldırı bilgileri, geçmiş saldırı bilgileri, sunuculara ait bilgiler ve saldırganlara ait bilgiler olmak üzere beş açıdan analiz edilmiştir. 2015 yılında ".mil.tr" ve ".pol.tr" uzantılı internet sitelerine saldırı olmadığı anlaşılmış; ".edu.tr" gibi farklı uzantılı kamu internet siteleri ise çalışmaya dâhil edilmemiştir.

Zone-H kayıtlarına göre 2015 yılında gerçekleşen 848 saldırının 204'ü tekil saldırı, 644'ü ise toplu saldırı şeklindedir. Toplu saldırı sayısının yüksek olması nedeniyle, saldırıya uğrayan internet sitelerinin büyük kısmının aynı IP adresi üzerinde yayın yaptığı anlaşılmaktadır. Bu durumun en önemli sebebi, özellikle aynı kuruma ait farklı hizmet, birim ve şubelere ait internet sitelerinin aynı IP adresi üzerinde ve (büyük çoğunluğunun) aynı etki alanı üzerinde farklı alt etki alanları ile yayın yapmasıdır.

Gerçekleştirilen 848 saldırının 225'i gibi önemli bir oranının internet sitesinin ana sayfasına yönelik olduğu görülmektedir. Toplum üzerinde kısa sürede daha fazla etki bırakılması amacı ile bilgisayar korsanları tarafından ana sayfa saldırılarına daha fazla önem verilmekte ve ana sayfa saldırıları prestij olarak değerlendirilmektedir.

Benzer şekilde saldırı gerçekleştirilen 848 internet sitesinin %35'inin (toplam 297 internet sitesi) geçmişte de saldırıya uğradığı anlaşılmaktadır. 2015 yılı Kasım ayında saldırıya uğrayan 107 internet sitesi arasında toplam beş defa saldırıya uğramış internet sitesinin bulunması ve 12 internet sitesinin üç ay içinde tekrar saldırıya uğramış olması; alınan/alınması gereken güvenlik tedbirlerinin tekrar gözden geçirilmesi gerektiğini göstermektedir. Diğer taraftan, aynı internet sitesine tekrar yapılan siber

saldırılarda saldırganların büyük kısmının farklı olması; bilgisayar korsanlarının saldırdıkları internet sitelerine tekrar saldırma konusunda özel bir çaba içinde olmadığını göstermektedir.

2015 yılında ülkemizde siber saldırı gerçekleştirilen kamu kurumlarının internet sitelerine ait sunucuların 774'ü Türkiye'de yayın yaparken, 74 sunucunun yurtdışında sekiz farklı ülkede bulunduğu anlaşılmaktadır. Bu durum, özellikle yurtdışında sunucunun bulunduğu şirket çalışanlarının maddi çıkar, tehdit, millî ve manevi duygular veya başka bir sebeple art niyetli eylemlerde bulunma riskini beraberinde getirmektedir. Bu açıdan başta ".gov.tr" uzantılı internet siteleri olmak üzere ülkemizde kamuya ait internet sitelerinin yurtdışından yayın yapmasına izin verilmemeli; böylece, siber saldırı ve bilgi sızma riskleri azaltılmalıdır.

Saldırıya uğrayan internet sitelerinin yayın yaptığı sunucuların 495'inin Windows işletim sistemi, 342'sinin ise Linux işletim sistemine sahip olduğu anlaşılmaktadır. Farklı işletim sistemleri üzerinde yayın yapılması konusunda bir değerlendirme yapılamamakla birlikte, işletim sistemlerinde bulunan açıklıkların kapatılabilmesi ve açıklık sebebiyle siber saldırı riskinin azaltılması amacıyla işletim sistemleri ve kullanılan uygulamaların düzenli olarak güncellenmesi gerekmektedir. Diğer taraftan, sunucudaki verilerin düzenli şekilde yedeklenmesi (*backup* alınması) saldırı zararlarını azaltacaktır.

2015 yılında ülkemizde kamu kurumlarına ait internet sitelerine yönelik gerçekleştirilen 848 saldırının 25 farklı ülkeden toplam 131 farklı bilgisayar korsanı/bilgisayar korsanları grubu tarafından gerçekleştirildiği anlaşılmaktadır. Bununla beraber bilgisayar korsanları tarafından yapılan kayıtlardan oluşan Zone-H verilerinde yer alan takma isimler, mesajlar, resimler ve videolarla doğrudan bir şahsı/grubu/ülkeyi sorumlu tutmak mümkün değildir. Bırakılan mesajlar ve yapılan paylaşımların hedef saptırma amaçlı olması mümkündür. Diğer taraftan, özellikle yurtdışından yapılan saldırıların tamamına yakınında ülkemiz açısından siyasi/politik yönünün bulunmadığı ve IP-tarama yöntemiyle rastgele seçilmiş hedef saldırısı olduğu değerlendirilmektedir.

Yapılan saldırıların %70'inin Türkiye merkezli olduğu görülmektedir. İnternet sitelerine bırakılan mesajların bir kısmının Türkiye

politikaları ve saldırıya uğrayan kamu kurumlarının uygulamaları ile ilgili olmadığı, saldırının siyasi bir yönünün bulunmadığı; "açıklarınızı kapatın" şeklinde uyarı biçimindeki mesajlardan veya ABD ve İsrail karşıtı söylemlerden anlaşılmaktadır. Diğer taraftan, saldırıların bir kısmında "Kürtlere özgürlük", "Kürdistan Katliamlarına Dur Diyeceğiz", "Serbest bilgi akışı engellenemez" gibi siyasi/politik mesajlar bulunduğu ayrıca terör örgütü PKK/KCK lehine resim ve video paylaşımlarının bulunduğu görülmektedir.

Siyasi/politik, ekonomik, ego, eğlence, millî ve manevi duygular gibi farklı motivasyonlara sahip bilgisayar korsanlarının en büyük ortak noktası; siber saldırı yapılacak hedeflerin kamu kurumlarına ait internet siteleri olmasıdır. Devletler sundukları hizmetleri internet ortamına aktardıkça (bilgi amaçlı internet sitesi oluşturma ve e-devlet hizmetleri gibi), bilişim sistemlerine bağlılıkları artmakta ve saldırıya açık hale gelmektedir. Bu bağlamda, bilişim teknolojilerini en fazla kullanan devletlerin siber saldırıya maruz kalma riskleri yüksek iken, internet ortamında düşük profilde faaliyette bulunan devletler için bu risk daha azdır. Gelişen teknolojik imkânlar, vatandaşların beklentisi ve vatandaş odaklı, şeffaf bir kamu yönetimi anlayışı ile ülkemizde de bilişim sistemlerine olan bağlılığın artacağı beklenmektedir. Bu artışa paralel olarak ülkemiz açısından siber saldırı riskinin de yükseleceği değerlendirilmektedir.

Summary

Information security protects information from unauthorized access, use, modification, or destruction. As a result of improvements in information technologies (IT) and dependency on IT systems, cyber attacks to IT systems have increased. Thus cyber security concept has become an important issue for all governments. Therefore, the aim of information security is defined as "to minimize the risk of exposing information."

In this study, cyber security is handled with the perspective of cyber attacks to websites. As the starting point, information security is mentioned and it is followed by "cyber security violations" and "hacker and hack culture" parts. In the third part, "the cyber attacks to the

websites with ".gov.tr" extensions of the governmental institutions in Turkey in 2015" is analysed by using 848 cyber-attack records which have been obtained from Zone-H (www.zone-h.org). The last part of the study is the conclusion of this examination.

The aim of cyber security is to protect IT systems and ensure information security. Cyber security has three crucial components as availability, integrity, and confidentiality. These components are important to ensure cyber security and all of them must be protected for violations. This concept is also valid and has an important role for the security of websites. Today, governments present a great number of public services via internet. The increase of services also brings with the risk of cyber attacks to websites. In this study, cyber attacks to websites are examined with the perspective of "integrity violations". Integrity violation, which is also known as web defacement, is a cyber attack to websites by changing the interface to face page, especially to black page.

Hacker is someone who searches and investigates the weaknesses of the IT systems, uses the exploits and accesses the systems as unauthorised user. Hack culture is a belief and consideration of hackers. In this study, hack culture is discussed in the subheadings as "crackers in hack culture", "privacy in hack culture", "publicity in hack culture", and "motivation in hack culture". Firstly, hacker and cracker are different terms. Their motivations and IT knowledge are not the same. Crackers use package software and access IT systems without much information. Also, their aims and motivation are usually to have fun, to prove themselves, and to gain money or reputation. On the other hand, hackers are well informed about computer technologies, network systems, programming languages, and social engineering. Most hackers attack a system with ideological, cultural, or political purposes. In hack culture, privacy is very important, because materialized action is not legal. For example, a study which was made in 2009 in Turkey about hackers showed that %65.1 of hackers knows that their actions are illegal. Moreover, announcing the cyber attack is another important concept in hack culture. Most hackers want to be recognized with nick or group names. For this reason, they save their records and publish them via websites, social media, and other platforms. The motivation in hack culture is

differed with hacker profile such as cyber terrorists, cyber warriors, hacktivists, malware writers, crackers, etc. Their motivation is categorized in three groups as political, economic and socio-cultural. The aim of this study is to give information about hack, hacker and hack culture as well as to analyse the cyber attacks to websites. Due to the fact that there is no official published data, the data in this study has been obtained from an open source. Zone-H is a public website on which attackers have saved their defacements since 2002. Their data is accessible with some little limitation.

In this study, the zone-h records have been filtered with ".gov.tr", which is the extension for government websites in Turkey. The total score is 8.998 from 2002 to the end of 2015. Due to the fact that a massive amount of data was listed, a re-filtering of the source with the dates between 01.01.2015 and 31.12.2015 has been performed and 848 records have been gathered. This study only focuses on government websites with the extensions of ".gov.tr". Websites with ".edu.tr" extensions and others have been ignored. The data has been analysed through five different perspectives as attack information by monthly, homepage defacement, attacks history, information about servers, and information about attackers.

After having analysed the 848 records, it has been seen that 204 defacements are "single IP defacement" and 644 of them are "mass defacement". It means that most of the government websites are serving with the same IP (same server). The single IP records are nearly same for all months with approximately 18 attacks per month. The number of attacks in July and August decreases relatively but it is not possible to make a decision.

Homepage defacements are more prestigious in hack culture. Mostly, subdomain attacks are not praiseworthy for people, so hackers want to attack the homepage. It is seen that 255 of 848 records belong to homepage defacements. Therefore, it can be said for most of the websites that attackers could not find any vulnerabilities and weaknesses in home directory.

After having analysed the 848 records, it is seen that 297 web sites which were attacked had also been attacked previously. It is also shown that almost all attackers who have attacked the same websites are different users. Thus, it can be said that attackers were not interested in re-attacking the websites which they had attacked previously. 107 of the records in November 2015 also show that 50 websites were attacked twice, six websites were attacked three times, two websites were attacked four times and one website was attacked five times in total. In addition to this, 12 attacks were materialized within three months. Therefore, it can be said that website admins do not review the cyber security preventions sufficiently after the defacements.

The study shows that all of the government websites are not located within Turkey. When the 848 website server locations are analysed, it is seen that there are eight different countries,, where website servers are located in. 774 websites are located within Turkey, others are located in Cyprus (30), the USA (18), Germany (16), the Netherlands (four), France (two), the UK (two), Canada (one) and Lithuania (one). When the server operating systems (OS) are analysed, it is seen that 495 servers have Windows OS, 342 serves have Linux OS and 11 servers have unknown operating systems.

According to fake names, messages, and the sharing of pictures and videos in Zone-H records, it has been made clear that the cyber attacks have been performed by 131 different hackers or hacker groups in 25 different countries. Additionally, this study shows that 70% of the origins of cyber attacks are based in Turkey and 35% of websites had been attacked previously.

Kaynakça

Kitaplar

AKDENİZ, Gökşin. "Hacker Etiği", (Der: Keleş, A.R. ve Sal, Y.), ***Hack Kültürü ve Hacktivizm: Yeni Bir Siyaset Biçimi,*** Alternatif Bilişim Derneği Yayını, İstanbul, 2013. 9-15.

BTK, ***Üç Aylık Pazar Verileri Raporu: 2015 Yılı 2. Çeyrek***, Bilgi Teknolojileri ve İletişim Kurumu, Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı, Ankara, 2015.

DENNING, Dorothy E. "Cyber Conflict as an Emergent Social Phenomenon", (Ed: Holt, T.J. ve Schell, B.H.), ***Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications***, IGI Global Press, PA, ABD, 2011, 170-186.

SACHIN, Vaidehi. ***Cyber Terror – The Hidden Crime***, Quality Printers: Hindistan, 2010.

Makaleler ve Kitap Bölümleri

ABLON, Lillian; LIBICKI, Martin C. and GOLAY, Andrea A., "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar", ***USA National Security Research Division***, 2014.

GÜRKAYNAK, Muharrem ve İREN, Adem Ali. "Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler", ***Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi***, 2011, 16 (2), 263-279.

HAN, Chen and DONGRE, Rituja. "What Motivates Cyber-Attackers?", ***Technology Innovation Management Review***, (Oct.2014), 40-42.

HEKİM, Hakan ve BAŞIBÜYÜK, Oğuzhan. "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", ***Uluslararası Güvenlik ve Terörizm Dergisi***, 2013, 4 (2), 135-158.

İLÇİN TUĞ, Emine; ADAK, Ş. Feyza ve ÇAKIR, Hüseyin. "Bilişim Güvenliği Tedbirleri ve TKDK Kurumunda Uygulama Örneği", ***Bilişim Teknolojileri Dergisi***, 2014, 7 (1), 11-18.

JURGENSON, Nathan. "Liquid Information Leaks", ***International Journal of Communication***, 2014, 8, 2651–2665.

KANTI, Tushar; RICHARIYA, Vineet and RICHARIYA, Vivek. "Implementation of an Efficient Web Defacement Detection Technique And Spotting Exact Defacement Location Using Diff Algorithm", ***International Journal of Emerging Technology and Advanced Engineering***, 2012, 2 (3), 252-256.

KAUR, Harkarandeep; SINGH, Er. Gurjot and KHURANA, Suman. "Analyzing Website Hacking Tool and Their Prevention Techniques", ***International Journal of Computer and Communication System Engineering***, 2015, 2 (3), 523-529.

KESER, Hafize ve GÜLDÜREN, Can. "Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme Çalışması", ***Kastamonu Eğitim Dergisi,*** 2013, 23 (3), 1167-1184.

LUSTHAUS, Jonathan. "Electronic Ghosts", ***Democracy Journal,*** 2013, 31, 45-57.

ÖĞÜN, Mehmet Nesip ve KAYA, Adem. "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler", ***Güvenlik Stratejileri Dergisi***, 2013, 18, 145-181.

SARASAN, Sandra. "Detection and Prevention of Web Application Security Attacks", ***International Journal of Advanced Electrical and Electronics Engineering,*** 2013, 2 (3), 29-34.

SHARMA, Aakashdeep and SINGH, Narinder. "Cyber Terrorism And Cyber Laws: The Challenge For Governments", ***IAHRW International Journal of Social Sciences Review,*** 2014, 2 (3).

TÜRKAY, Şeyda. "Siber Savaş Hukuku Ve Uygulanma Sorunsalı", ***İstanbul Üniversitesi Hukuk Fakültesi Mecmuası***, 2013, 71 (1), 1177-1228.

UÇKAN, Özgür. "Dijital Aktivizmin Sınır Boyunda Hacktivizm: Anonymous ve RedHack Örnekleri", (Der: Keleş, A.R. ve Sal, Y.), ***Hack Kültürü ve Hacktivizm: Yeni bir Siyaset Biçimi,*** Alternatif Bilişim Derneği Yayını, İstanbul, 2013A, 53-79.

UÇKAN, Özgür. "Hacker'lar: Viral Kültürün "Semantik Gerillalar"ı mı, Enformasyon Toplumunun Veri Hırsızları mı?", (Der: Keleş, A.R. ve Sal, Y.), ***Hack Kültürü ve Hacktivizm: Yeni bir Siyaset Biçimi,*** Alternatif Bilişim Derneği Yayını, İstanbul, 2013B, 41-47.

YEGEN, Ceren. "Dijital Aktivizmin Bir Türü Olarak Hacktivizm ve "RedHack", ***Intermedia Uluslararası Hakemli İletişim Bilimleri E-Dergisi***, 2014, 1 (1), 118-132.

WORI, Okechukwu. "Computer Crimes: Factors of Cybercriminal Activities", ***International Journal of Advanced Computer Science and Information Technology***, 2014, 3 (1), 51-67.

Bildiriler

AKKAYA, Mariye Umay. Siber Güvenlik Standartları ve Belgelendirmeleri, ***ICSG İSTANBUL 2014-Uluslararası İstanbul Akıllı Şebekeler ve Şehirler Kongre ve Fuarı,*** 8-9 Mayıs 2014, Bildiri Kitabı, İstanbul, 2014, ss:48-52.

BORGOLTE, Kevin; KRUEGEL, Christopher and VIGNA, Giovanni. "Meerkat: Detecting Website Defacements Through Image-Based Object Recognition", ***24th USENIX Security Symposium***, 12-14 August 2015, Washington, DC, USA.

DOĞU, Ali Haydar. "İdarelerin İnternet Sitelerinden Doğan Sorumlulukları", ***18. Türkiye'de İnternet Konferansı***, 9-11 Aralık 2013, İstanbul Üniversitesi, İstanbul, 2013.

FURNELL, Steven M. "The Problem of Categorising Cybercrime and Cybercriminals", ***2nd Australian Information Warfare and Security Conference***, 29-30 November 2001, Perth, Western Australia.

Tezler

ERİŞ, Ufuk. "Türkiye'de Kırıcı (Hacker) Kültürü", Anadolu Üniversitesi Sosyal Bilimler Enstitüsü Eskişehir, 2009, (Yayımlanmamış Doktora Tezi).

KARA, Mahruze. Siber Saldırılar - Siber Savaşlar ve Etkileri, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2013, (Yayımlanmamış Yüksek Lisans Tezi)

SAMUEL, Alexandra Whitney. "Hacktivism and the Future of Political Participation", Harvard University Department of Government, Cambridge, USA, 2004 (Yayımlanmamış Doktora Tezi)

SAYAR, Özgür. "Türkiye'de ve Dünyada Elektronik Devlet Uygulamaları Bağlamında Risk Faktörleri", Beykent Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2007 (Yayımlanmamış Yüksek Lisans Tezi).

İnternet Kaynakları

CVE Details İnternet Sitesi, 2015, "Top 50 Products By Total Number Of "Distinct" Vulnerabilities", https://www.cvedetails.com/top-50-products.php, (Erişim Tarihi: 10.12.2015).

HENG, Christopher. 2014, "Should You Choose a Linux or a Windows Web Hosting Package? And Is There Such a Thing as a Mac Web Host?", http://www.thesitewizard.com/webhosting/linux-vs-windows.shtml, (Erişim Tarihi: 10.12.2015).

HP İnternet Sitesi. 2013, "Analysis of an Automated Mass Hack and Defacement Exploiting CVE-2013-5576", http://community.hpe.com/t5/Security-Research/HP-Security-Research-Threat-Intelligence-Briefing-Episode-8/ba-p/6248499, (Erişim Tarihi: 01.12.2015).

Kalkınma Bakanlığı İnternet Sitesi. "2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı", Kalkınma Bakanlığı, Bilgi Toplumu Dairesi Başkanlığı, www.bilgitoplumustratejisi.org. (Erişim Tarihi: 01.12.2015).
Türk Dil Kurumu İnternet Sitesi. "Güncel Türkçe Sözlük", www.tdk.gov.tr, (Erişim Tarihi: 08.12.2015).
Zone-H İnternet Sitesi. Special Defacement, http://www.zone-h.org/archive/special=1, (Erişim Tarihi: 10.11.2015 ve 01.01.2016).