Nesnelerin İnternetinin Güvenliğinde İnsan Faktörü

Human Factors in Internet of Things Security

Mevlüt Serkan TOK
TOBB ETÜ
Bilgisayar Mühendisliği Bölümü
mtok@etu.edu.tr
ORCID: 0000-0002-5048-8409

Ali Aydın SELÇUK
TOBB ETÜ
Bilgisayar Mühendisliği Bölümü
aselcuk@etu.edu.tr
ORCID: 0000-0002-8963-1647

Öz

İnternete bağlı nesneler ulaşım, sağlık, enerji gibi sektörler ile akıllı bina vb. uygulamalarda yoğun olarak kullanılmaktadır. Bu nesneler otomasyon ve maliyet avantajlarının yanı sıra yenilikçi iş modelleri ve kullanıcı deneyimleri sunmaktadır. Kullanıcıların internete bağlı nesnelerin konfigürasyonlarında basit parolalar seçmesi veya bu cihazlarla birlikte gelen varsayılan parolaları değiştirmemeleri ciddi güvenlik açıkları yaratmaktadır. Son yıllarda Mirai vb. zararlı yazılımlar bu açıklıkları sömürerek çevrim içi nesneleri ele geçirmekte ve dağıtık servis dışı bırakma saldırılarında saldırı unsuru olarak kullanarak hizmet kesintilerine, maddi kayıplara ve itibar zedelenmesine neden olmaktadır. Bu çalışmada kullanıcıların nesnelerin internetine yönelik güvenlik ve risk algılarının, parola kullanımı ve güvenliğine dair tercihlerinin tespit edilmesi ve insan faktörünün nesnelerin interneti cihazlarının güvenliğindeki öneminin ortaya konulması amaçlanmıştır. Katılımcılardan anket yöntemi ile veri toplanarak elde edilen bulgular tartışılmış, Türkiye pazarında nesnelerin interneti cihazlarının tekil olmayan varsayılan parolalar ile kullanıcılara arzını engelleyecek tedbirler önerilmiştir.

Anahtar Sözcükler: *nesnelerin interneti, siber güvenlik, parola güvenliği, mirai, insan faktörü*

Abstract

The growing presence of Internet of Things (IoT) devices has not only contributed in digital transformation of industry, transportation, healthcare and many other fields with smart devices producing and sharing data online; but also provided innovative business models and novel user experiences. Configuring internet of things (IoT) devices with easy or default passwords leads to serious vulnerabilities. In recent years, malware (Mirai etc.) which are capable of creating IoT botnets and organizing distributed denial of service (DDoS) attacks have given rise to service disruptions, reputational and financial loss. In this study, we aimed to emphasize importance of human factor in IoT device security. To determine users' perceptions of security and risks related to IoT devices, preferences of password usage and password security; a questionnaire was employed to collect data and findings were discussed. Some measures to prevent circulation of IoT devices with common default passwords in Turkish market were proposed.

Keywords: *internet of things, cyber security, password security, mirai, human factor*

Gönderme ve kabul tarihi: 17.10.2019-17.11.2019
Makale türü: Araştırma

1. Giriş

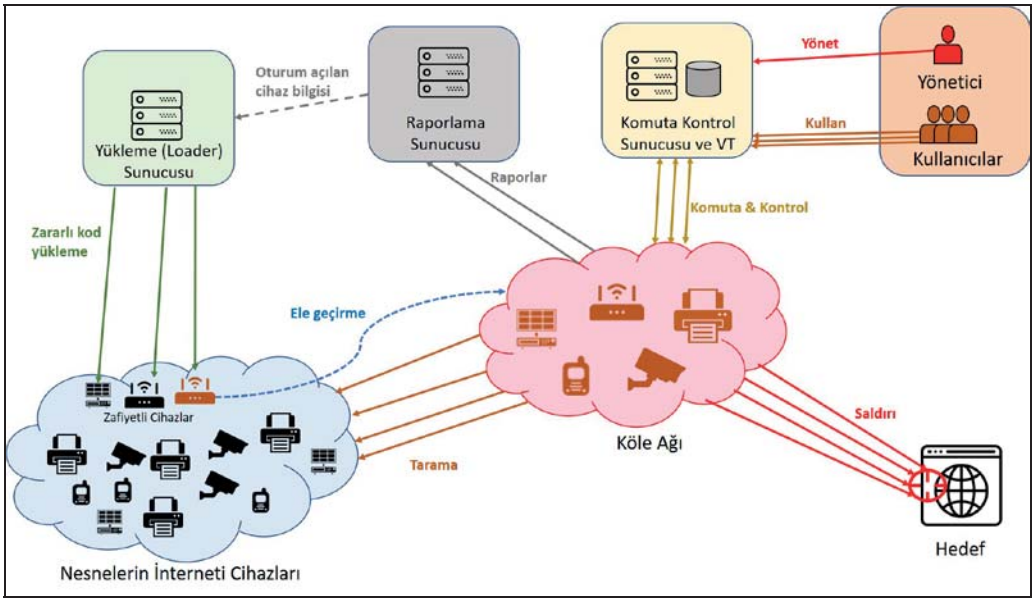
Bilgi teknolojilerinin her geçen gün hayatımızda daha fazla yer alması ile internete bağlı, veri alabilen ve gönderebilen nesnelerin kullanımı da yaygınlaşmıştır. Nesnelerin interneti (internet of things - IoT) olarak da adlandırılan bu ekosistem sayesinde neredeyse her bireyin yakın çevresinde çeşitli amaçlarla kullanılan en az bir çevrim içi nesne bulabilmek mümkündür [1]. 2030 yılına kadar internete bağlı nesnelerin sayısının 500 milyarı aşması beklenmektedir [2]. Geniş kullanım alanı bulunan çevrim içi nesneler siber saldırıların hem faili hem de hedefi olabilmektedir. OWASP tarafından yayınlanan 2018 yılı nesnelerin internetini tehdit eden ilk on zafiyet listesinde nesnelerin

yönetiminde basit, tahmin edilir, herkesçe erişilebilen veya değiştirilemez parola kullanımı ilk sırada bulunmaktadır [3].

20 Eylül 2016'da KrebsOnSecurity isimli siber güvenlik konulu bir blog sitesi 620 GBps'ye ulaşan boyutta dağıtık hizmet dışı bırakma saldırısına (distributed denial of service-DDoS) uğramıştır. Bu boyutta bir saldırının, o güne kadar yapılmış en büyük dağıtık hizmet dışı bırakma saldırısının yaklaşık iki katı olduğu değerlendirilmiştir [4]. Mirai botnet olarak da adlandırılan bu saldırıya dair kaynak kodları 30 Eylül 2016'da HackForums.net örün sitesinde "Anna-senpai" kullanıcı adlı bir şahıs tarafından yayınlanmıştır [5]. 21 Ekim 2016'da dinamik DNS sağlayıcısı olan Dyn'e yapılan saldırının boyutunun 1.2 TBps'ye ulaştığı tespit edilmiştir ki kendi türünün en büyük boyuttaki saldırısı olmasının yanı sıra önemli sayıda internet sitesinin hizmet dışı kalmasına yol açmıştır. Dyn bu saldırıya katılan uç sistem sayısının 100.000 civarında olduğunu duyurmuştur [6]. Mirai zararlı yazılımının mantıksal yapısı Şekil 1'de gösterilmiştir.

2. Art alan

Mirai zararlı yazılımının orijinal versiyonunun kaynak kodu incelendiğinde kodların üç ayrı bölümde (Bot, Loader, CNC) toplandığı, bot ve loader bölümlerinin C dili, CNC bölümünün ise Go dili ile yazıldığı görülmektedir [7]. Kaynak kodları içerisinde şifrelenerek kodlanmış ve root:root, admin:root, guest:guest vb. yaygın şekilde kullanılan 60 farklı kullanıcı adı:parola çifti kayıtlıdır. İçerisinde bulunan scanner isimli modül ile rastgele IP adresleri üretmekte, üretilen adresleri ABD Savunma Bakanlığı vb. bir kısım organizasyonların IP adreslerini içeren bir kara listeyle kıyaslayarak bu organizasyonları kapsam dışında bırakmaktadır [8]. Üretilen IP adresinin 23 ve 2323 portlarına bağlantı talebi göndererek Telnet protokolü açık mı kontrol edilmekte, açık olduğu takdirde kayıtlı parola çiftlerini kullanarak kaba kuvvet saldırısı yapılarak Telnet bağlantısı kurulmakta, oturum açma bilgileri raporlama sunucusuna gönderilmekte ve yükleyici adı verilen bir sunucu tarafından cihaza yüklü BusyBox uygulaması sömürülerek önceden hazırlanmış ikili kodlar cihaza yüklenmekte ve cihaz köle ağına dahil edilmektedir [9].



Şekil-1: Mirai zararlı yazılımının mantıksal yapısı.

Köle ağına dahil edilen cihazlar üzerinden hedef örün sitelerine DNS flood, SYN flood, ACK flood,

PSH flood, HTTP flood teknikleri ile dağıtık hizmet dışı bırakma saldırısı yapabilmek mümkündür [10]. Mirai ve türevleri tarafından ele geçirilen cihazlar arasında şu ana kadar yönlendiriciler, dijital video kaydediciler, IP kameralar ve yazıcılar bulunmaktadır [11]. Pazar payı ve tasarım unsurları göz önünde bulundurularak farklı cihazları ele geçirecek varyantlar kodlamak mümkündür [12].

Mirai'nin orijinal versiyonunda sadece açık (public) IP adresine sahip cihazlar etki altına alınmışken Hajime gibi daha gelişmiş versiyonları Evrensel Tak-Çalıştır (UPnP- Universal Plug and Play) İnternet Ağ Geçidi Cihazı (IGD-Internet Gateway Device) protokolünü destekleme yeteneği kazanmış ve bir yönlendirici arkasındaki yerel IP adresine sahip cihazları da tehdit eder hale gelmiştir [13].

Mirai'nin kaynak kodlarının yayınlanması onu adeta bir zararlı yazılım şablonu haline getirmiştir [14]. Mirai'nin kaynak kodlarının yayınlanmasından sonra kötü niyetli kişilerce geliştirilerek kullanılmasına devam edilmiştir [15]. Bu durum Mirai tabanlı zararlı yazılım çeşitliliğini arttırmış ve yeni bir varyantın ortaya çıkma süresini kısaltmıştır [16]. 2017 yılında işletilen bal küpü tuzaklarında 371 farklı parola ve 1028 farklı ikili kodun ele geçirilmesi, farklı portlar ve protokoller üzerinden bağlantı taleplerinin tespiti Mirai'nin evrimleşme hızının bir göstergesidir [17]. 2018 yılında tespit edilen zararlı trafiğin %78'ini nesnelerin interneti kapsamında bulunan, ele geçirilmiş cihazların oluşturduğu köle ağların meydana getirdiği ve bu ağları oluşturan zararlı yazılımların en az %35 oranında Mirai ile benzer kaynak kodları kullandığı tespit edilmiştir [18]. 2019 yılı mart ayı itibariyle Mirai ardılı zararlı yazılımlar çeşitli açıklıkları sömürmenin yanı sıra varsayılan parola kullanıma yönelik kaba kuvvet saldırısı yapmaya devam etmiştir [19]. 2019 yılı nisan ayı itibariyle Huawei ve Linksys markalı yönlendiriciler Mirai zararlı yazılımının evrimleşmiş versiyonlarınca siber saldırıya uğramış ve bu saldırılarda eski tarihli açıklıklar da sömürülmüştür [20].

2019 yılı haziran ayı itibariyle dünya çapında 23 numaralı portu açık ve içerisinde Busybox uygulaması kurulu toplam 6.132.907 cihaz bulunduğu ve bunların 126.903 adedinin Türkiye lokasyonlu olduğu; Mirai komuta kontrol sunucularının desteklediği protokoller, dosya yapısı ve parmak izi dikkate alınarak yapılan sorgulamalarda halen faal durumda olan yaklaşık 1000 sunucunun olduğu ve bunların yarısının ABD'de, 2 tanesinin Türkiye'de bulunduğu tespit edilmiştir [21]. Dolayısıyla halen zaaflı cihazların kullanımına ve botnet oluşturmaya devam edildiğini değerlendirmek mümkündür.

ABD siber olaylara müdahale birimince Mirai vb. zararlı yazılımlara karşı alınacak ilk tedbirin tüm varsayılan parolaların güçlü parolalar ile değiştirilmesi olduğu duyurulmuştur [22]. Varsayılan parola kullanımının yarattığı güvenlik açıklarının giderilmesi amacıyla bir kısım firmalar yeni üretilen ürünlerinde varsayılan parola uygulamasını kaldırmış ve sınırlı miktardaki ürüne güncelleme yayınlamıştır. Ancak güncellenmeyen ikinci el ürünlerin çeşitli siteler üzerinden satışına ve son kullanıcı tarafından kullanımına devam edilmektedir. ABD Kaliforniya eyalet senatosu tarafından yayınlanan bir yasa tasarısı [23], İngiliz Ticaret Bakanlığı tarafından yayınlanan bir yönetmelik [24] ile bu ülkelerde üretici ve satıcıların piyasaya sunduğu her bir çevrimiçi nesnenin varsayılan parolasının benzersiz olması zorunlu hale getirilmiş, Avrupa Telekomünikasyon Standartları Enstitüsü tarafından yayınlanan ETSI TS 103 645 "Cyber Security for Consumer Internet of Things" standartı ile tüketiciye sunulan nesnelerin interneti cihazlarının güvenli tasarımına yönelik temel ilkeler tespit edilmiştir [25]. Eylül 2016'da Türkiye'den 13.780 cihaz Mirai tarafından ele geçirilmesine ve enfekte olmuş cihaz barındıran ülkeler listesinde yedinci sırada olunmasına rağmen [17], ülkemizde henüz ortak bir varsayılan parola ile yapılandırılmış ağ erişim yetenekli nesnelerin ithalatını veya satışını engelleyen yasal bir düzenleme bulunmamaktadır.

Bu çalışmada, kullanıcıların nesnelerin güvenliğine dair algı ve eğilimlerini tespit ederek Mirai vb. zararlı yazılımlara karşı bilgi ve hazırlık düzeyini değerlendirmek amacıyla, 407 sosyal medya kullanıcısının gönüllü olarak katıldığı bir çevrim içi anket vasıtasıyla veri toplanmış ve elde edilen bulgular tartışılmıştır.

3. İlgili çalışmalar

2016 yılında ESET şirketi ve ABD Ulusal Siber Güvenlik Birliği (NCSA) tarafından gerçekleştirilen bir çalışmada 1527 katılımcının %22'sinin evinde 4-7 cihazın internet erişiminin olduğu, %29'unun evlerindeki modemin varsayılan parolasını değiştirmediği, katılımcıların %24'ünün evlerindeki termostatın kontrolü vb. amaçlar için mobil uygulama kullandığı, %85'inin web kameraların yetkisiz kişilerce erişilebilir olduğunun farkında

olduğu ve %36'sının web kameralarını korumaya dönük herhangi bir tedbir almadığı tespit edilmiştir [26].

2017 yılında 200 katılımcının akıllı televizyonlara yönelik mahremiyet ile ilgili risklere dair farkındalığını ölçmek amacıyla yürütülen bir çalışmada genel olarak düşük seviyede bir farkındalık olduğu görülmüş, katılımcıların %16'sının risklere dair farkındalık sahibi olduğu tespit edilmiştir. Akıllı televizyonun kullanılabilirlik seviyesini düşürmediği sürece mahremiyetin korunmasına dair alınacak tedbirlerin kullanıcılar tarafından benimseneceği sonucuna varılmıştır [27].

2019 yılı mart ayı içerisinde yayınlanmış bir çalışmada 158 katılımcıya çevrim içi anket uygulanmış ve katılımcıların %44'ünün herhangi bir internete bağlı nesneye sahip olmadığı, %36'sının bir nesneye, %20'sinin iki veya daha fazla sayıda nesneye sahip olduğu görülmüştür. Katılımcıların çoğunluğu güvenlik (%65) ve mahremiyetin (%63) internete bağlı bir nesnenin sahip olması gereken özelliklerden olduğunu belirtmiştir. İnternete bağlı bir nesnenin sahip olması gereken özelliklerin önem derecesine göre sıralanması sorusunda ise katılımcıların çoğunluğunun (%34) kurulum kolaylığı, kullanım kolaylığı, uygunluk, güvenlik ve mahremiyet yerine maliyet özelliğini ilk sırada seçtiği tespit edilmiştir. Bu durum "kullanıcılar tarafından teorik olarak güvenlik ve mahremiyete önem verilse de pratikte maliyetin daha önemli bir faktör olarak görüldüğü" şeklinde yorumlanmıştır [28].

Türkiye'deki bilgisayar kullanıcılarının bilgi güvenliğine dair genel farkındalık seviyelerini ölçmek amacıyla çok sayıda çalışma yapılmıştır [29]-[31]; ancak bu çalışmalar incelendiğinde genellikle üniversite vb. bir organizasyon bünyesinde kısıtlı bir evreni temsil eden örneklem ile icra edildiği görülmektedir. Yapılan literatür taramasında ülkemizdeki kullanıcıların nesnelerin internetine dair güvenlik algısını veya farkındalık düzeyini ölçen bir çalışmaya rastlanılmamıştır.

4. Yöntem

Katılımcılar

Araştırma 23-27 Nisan 2019 tarihleri arasında yürütülmüştür. Araştırmanın katılımcılarını sosyal medya kullanıcısı bireyler oluşturmaktadır. Katılımcılara ait demografik dağılım Çizelge-1'de sunulmuştur.

Çizelge-1: Katılımcıların Demografik Dağılımı

Değişken	Kategori	f	%
Cinsiyet	Erkek	217	53.32
	Kadın	190	46.68
Yaş	18-20	61	14.99
	21-30	194	47.67
	31-40	124	30.47
	41-50	25	6.14
	51-60	3	0.74
	61 ve üzeri	0	0
Eğitim durumu	İlkokul	1	0.25
	Ortaokul	5	1.23
	Lise	44	10.81
	Ön lisans	32	7.86
	Lisans	227	55.77
	Yüksek Lisans	66	16.22
	Doktora	32	7.86
Eğitim veya çalışma alanı bilgi teknolojileri / siber güvenlik ile ilgili mi?	Hayır	353	86.73
	Evet	54	13.27

2018 yılında Türkiye'de 51 milyon sosyal medya kullanıcısı olduğu [32] göz önünde bulundurularak %95 güven düzeyinde ve %5 hata payı dikkate alındığında 385 katılımcıdan oluşan bir örneklemin sosyal medya kullanıcılarını temsil edebileceği değerlendirilmiştir. Gönüllülük esasına göre toplam 533 kullanıcı araştırmaya katılmış, 407 kullanıcı araştırmayı tamamlamıştır. Katılımcıların araştırmayı tamamlama oranı %76'dır. Katılımcılar www.facebook.com, www.linkedin.com, www.twitter.com, www.eksisozluk.com örün siteleri üzerinden, erişim linki içerir davet metni paylaşılması suretiyle araştırmaya davet edilmiştir. Katılımcıların araştırmaya katılımını teşvike yönelik herhangi bir motivasyon (ödeme vb.) sağlanmamıştır.

Veri toplama aracı

Anketler ucuz bir yöntem olması ve mevcut davranışların tespiti hususunda veri toplamaya uygunluğu nedeniyle tercih edilmektedir [33]. Bu çalışmada birincil veriler çevrimiçi anket vasıtasıyla toplanmıştır. Araştırma tarama modeli kullanılarak gerçekleştirilmiştir. Anketin geliştirilmesinde alan yazındaki benzer araştırmalardan faydalanılmıştır.

Anket üçüncü taraf bir örün sitesi üzerinden gerçekleştirilmiştir. Mobil cihazlar ve bilgisayar üzerinden ankete katılım sağlanmış, site tarafından tutulan çerez bilgisi ile aynı cihazlardan katılım engellenmiştir. Anket öncesinde katılımcılardan e-posta adresi vb. kişisel bilgiler talep edilmemiş, anket müddetince IP adresi bilgisi tutulmamıştır. Her bir katılımcıya ankete katıldığı andan itibaren bir kimlik numarası atanmış ve yanıtlar bu kimlik numarası satırına kaydedilmiştir. Anket başlangıcında katılımcılara aydınlatılmış onam metni vasıtasıyla bilgi verilmiş ve gönüllü rızaları alınmıştır. Anket sonunda anlık istatistiksel sonuçlar katılımcılara gösterilmiştir. Anket toplam on altı sorudan oluşmaktadır. Kullanıcıların demografik bilgileri dört soruda, işletim sistemi ve web tarayıcı tercihleri iki soruda, parola kullanımı ve güvenliğine dair eğilimler beş soruda, nesnelerin interneti ve siber güvenlik konusundaki eğilimler dört soruda ölçülmüştür. Katılımcılardan isteğe bağlı beyan edilen görüş ve öneriler açık uçlu cevap verilen son soruyla toplanmıştır. Ankette toplamda dokuz adet çoktan seçmeli (tek cevaplı), beş adet çoktan seçmeli (çok cevaplı), bir adet sıralama, bir adet açık uçlu soru sorulmuştur.

Verilerin analizi

Veriler; sonuçların analizi ve iki değişkenli Ki-Kare testi olarak iki temel kategori altında analiz edilmiştir. Tüm analizler IBM SPSS Statistics V.22 yazılımı ile gerçekleştirilmiştir.

Ankette yer alan maddelerin toplandığı üç ana başlık olan işletim sistemi ve web tarayıcı tercihleri, parola kullanımı ve güvenliğine dair eğilimler, nesnelerin interneti ve siber tehdit algıları ile ilgili soruların yanıtları yüzde ve frekans ile betimlenmiştir.

Bilgi teknolojileri veya siber güvenlik konusunda eğitim görmüş veya bu alanlarda çalışan katılımcılar "bilgi sahibi katılımcı" olarak sınıflandırılmış ve bu kişilerin yanıtlarının diğer katılımcıların yanıtlarıyla ne kadar farklılaştığı Ki-Kare testi ile incelenmiştir.

5. Bulgular

İşletim sistemi ve web tarayıcı tercihleri

Katılımcıların büyük çoğunluğu (%91,1) bilgisayarlarında işletim sistemi olarak öncelikle Windows dağıtımlarını tercih etmiştir. Örün siteleri ziyaretlerinde katılımcıların çoğunlukla (%86,67) Google Chrome web tarayıcısını kullandıkları tespit edilmiştir. Katılımcıların işletim sistemi ve web tarayıcı tercihlerinin tespitine yönelik sorulan sorular ve verilen yanıtlar Çizelge-2'de sunulmuştur.

Çizelge-2: İşletim Sistemi ve Web Tarayıcı Tercihleri

Soru		f	%
S5 - Bilgisayarınızda hangi işletim sistemini kullanıyorsunuz? (Birden fazla seçeneği işaretleyebilirsiniz.)	Windows dağıtımları	369	91,11
	Mac OS	58	14,32
	Linux dağıtımları	27	6,67
S10 - Bilgisayarınızda hangi web tarayıcıyı kullanıyorsunuz? (Birden fazla seçeneği işaretleyebilirsiniz.)	Google Chrome	351	86,67
	Mozilla Firefox	122	30,12
	Opera	87	21,48
	Internet Explorer	75	18,52
	Safari	57	14,07
	Yandex	41	10,12
	Microsoft Edge	29	7,16
	TOR	27	6,67

Parola kullanımı ve güvenliğine dair eğilimler

Katılımcıların parola kullanımına ve güvenliğine dair algı ve tercihlerini belirlemek amacıyla toplam altı adet soru sorulmuştur.

Katılımcılardan günlük yaşantılarında kullandıkları altı ayrı parolayı önem derecesine göre sıralamaları istenmiştir. En önemli parola olarak internet bankacılık parolası seçilmiş; sırasıyla e-posta hesabı parolası, sosyal medya hesabı parolası, evlerindeki yönlendiricinin (modem) yönetici parolası, takip edilen bir forum sitesinin parolası ve tekrar girmeyi düşünmedikleri bir sitenin parolası katılımcılarca önemli görülmüştür.

Parola türlerinin katılımcılarca belirlenmiş sırası göz önünde bulundurularak (1) numaralı denklem ile her bir parolanın önem skoru hesaplanmıştır.

$$S_a = \frac{6*k_1+5*k_2+4*k_3+3*k_4+2*k_5+1*k_6}{\sum_{i=1}^{n} k_i} \quad (1)$$

S_a a parolasının skorunu, k_i a parolasını i. önem derecesine sahip parola olarak seçen katılımcı sayısını temsil etmektedir. Hesaplanan önem skorları Şekil-2'de sunulmuştur.

Katılımcıların çoğunluğu bir parolanın güçlü olmasının (%79,01) ve hatırlanmasının kolay olmasının (%45,19) parola seçiminde en önemli faktör olduğunu düşünmektedir. Katılımcıların %47,65'i, kendilerine gösterilen beş ayrı paroladan "7ujMko0admin" parolasını en güvenli parola olarak seçmiştir. "SEays214." parolası katılımcıların %46,67'si tarafından en güvenli parola olarak tercih edilmiştir. Katılımcıların çoğunluğu (%65,43) parola seçerken halen kullandığı birkaç parola bulunduğunu ve bu parolalar arasından seçim yaptığını beyan etmiş, katılımcıların çoğunluğu (%69,63) parolalarını saklama yöntemi olarak akılda tutma seçeneğini tercih etmiştir. Katılımcıların parola kullanımı ve güvenliğine dair eğilimlerinin tespitine yönelik sorulan sorular ve verilen yanıtlar Çizelge-3'te sunulmuştur.

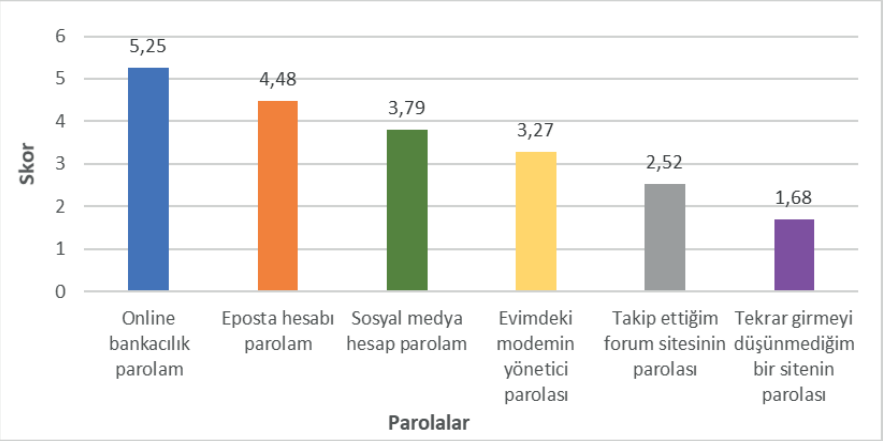
Nesnelerin interneti ve siber tehdit algıları

Katılımcıların nesnelerin internetinin güvenliği ve siber tehdit algılarını tespit etmek amacıyla sorulan dört adet soruya verilen yanıtlar Çizelge-4'te sunulmuştur. Katılımcıların %59,51'inin satın aldıkları modem, IP kamera vb. bir cihazla birlikte verilen parolayı cihazın ilk kurulumu esnasında değiştirirken %29,14'ünün varsayılan parolayı değiştirmeden sürekli kullandığı belirlenmiştir. Katılımcıların bildiği görülmüştür. Katılımcıların %75,56'sının modem (yönlendirici) cihazının bir siber saldırıya maruz kalabileceğini bildiği, %44,44'ünün kablosuz yazıcıların siber saldırıya maruz kalabileceğini bildiği tespit edilmiştir.

Bilgi sahibi katılımcı yanıtlarının diğer katılımcı yanıtlarıyla karşılaştırılması

Araştırmaya katılan bireylere bilgi teknolojileri veya siber güvenlik üzerine eğitim alıp almadıkları veya bu alanda çalışıp çalışmadıkları sorularak bilgi teknolojileri ve siber güvenlik konusunda bilgi sahibi olduğu değerlendirilen bireyler tespit edilmiş ve kısaca "bilgi sahibi katılımcı" olarak sınıflandırılmıştır. Toplanan yanıtların kategorik veri olmaması nedeniyle iki soru Ki-Kare testine tabi tutulmadan Çizelge-5'te görüldüğü üzere çapraz karşılaştırma yapılmış, beş soruya verilen yanıtlar ise düzenlenerek katılımcıların verdikleri yanıtların bilgi sahibi olma değişkenine göre çaprazlanması ile Ki-Kare testi gerçekleştirilmiş ve dağılımlar arasında istatistiksel açıdan anlamlı fark bulunup bulunmadığı tespit edilmiştir.

Bilgi sahibi katılımcıların bir örün sitesine siber saldırı yapabilecek cihazları doğru seçme oranının diğer katılımcılara oranla daha yüksek olduğu görülmüştür. Benzer bir şekilde bu katılımcıların siber saldırıya maruz kalabilecek cihazları tespit etme oranının diğer katılımcılara oranla daha yüksek olduğu görülmüştür.



Şekil-2: Katılımcıların parola önem sıralaması sonucu hesaplanan önem skorları.

Çizelge-3: Parola Kullanımına Dair Algı ve Tercihler

Soru		f	%
S12 - Sizce bir parola seçiminde en önemli faktör nedir? (Birden fazla seçeneği işaretleyebilirsiniz.)	Güçlü olmalı (zor tahmin edilmeli)	320	79,01
	Hatırlaması kolay olmalı	183	45,19
	Eğlenceli veya ilginç olmalı	26	6,42
	Kısa olmalı, kolay yazılmalı	13	3,21
	Diğer	13	3,21
S13 - Sizce aşağıdaki parolalardan hangisi en güvenli paroladır?	7ujMko0admin	193	47,65
	SEays214.	189	46,67
	Nisan2019.	10	2,47
	147258	9	2,22
	I love you2	4	0,99
S14 – Parolalarınızı nasıl seçersiniz?	Kullandığım birkaç parolam var, onların arasından seçerim.	265	65,43
	Her hesap için ayrı parola seçerim	69	17,04
	Çoğunlukla ayrı parolalar seçerim, bunlar nadiren birbirinin aynı olabilir.	45	11,11
	Hepsi aynı paroladır.	26	6,42
S15 – Parolalarınızı çoğunlukla nasıl saklamayı tercih edersiniz?	Aklımda tutarım.	282	69,63
	Bilgisayarımda veya cep telefonumda bir dosya üzerine kaydederim.	49	12,1
	Kâğıda, post-it vb. fiziksel bir ortama yazarım.	29	7,16
	Web tarayıcıma hatırlaması için kaydederim.	20	4,94
	Parola yönetim programı kullanır ve ona kaydederim.	23	5,65
	Diğer	2	0,49

Çizelge-4: Nesnelerin İnterneti ve Siber Tehdit Algısı

Soru		f	%
S4 - Satın aldığınız bir cihazla verilen örn. yönlendirici (modem), IP kamera vb. ile birlikte verilen yönetici parolasını (örn. admin, root vb.) ne kadar süreyle kullanırsınız?	Kullanmadan ilk kurulumda değiştiririm.	241	59,51
	1 aya kadar kullanırım.	4	0,99
	3 aya kadar kullanırım.	12	2,96
	6 aya kadar kullanırım.	30	7,41
	Sürekli kullanırım.	118	29,14
S6 - Bir siber saldırının hedefi olma ihtimalinizi 1-5 arasında puanlayınız. (5 en yüksek ihtimal)	1-Hedef olma ihtimalim yoktur.	68	16,79
	2-Hedef olma ihtimalim azdır.	184	45,43
	3-Hedef olup olmama ihtimalim aynıdır.	112	27,65
	4-Hedef olma ihtimalim yüksektir.	20	4,94
	5-Kesinlikle hedefim.	21	5,19
S9 - Aşağıdaki cihazlardan hangileriyle bir web sitesine siber saldırı yapılabilir? (Birden fazla seçeneği işaretleyebilirsiniz.)	Yönlendirici (modem)	267	65,93
	IP kamera	174	42,96
	Kablosuz bebek monitörü	91	22,47
	Dijital video kayıt cihazı (DVR)	86	21,23
	Kablosuz yazıcı	82	20,25
	TV uzaktan kumandası	28	6,91
	Fotoselli lamba	18	4,44
S11 - Aşağıdaki cihazlardan hangileri siber saldırılara maruz kalabilir? (Birden fazla seçeneği işaretleyebilirsiniz.)	Yönlendirici (modem)	306	75,56
	Akıllı televizyon	295	72,84
	IP kamera	279	68,89
	Kablosuz bebek monitörü	183	45,19
	Kablosuz yazıcı	180	44,44
	Akıllı buzdolabı	174	42,96
	Mutfak robotu	27	6,67
	Elektrikli süpürge	20	4,94

Çizelge-5: Bilgi Sahibi Olma Değişkenine Göre Yanıtların Karşılaştırması

Soru		Bilgi sahibi katılımcı mı? Evet (%)	Hayır (%)
S9 - Aşağıdaki cihazlardan hangileriyle bir web sitesine siber saldırı yapılabilir?	Modem	83,3	62,8
	Dijital video kayıt cihazı	31,4	19,5
	Kablosuz bebek monitörü	35,1	20,3
	IP kamera	53,7	41
	Kablosuz yazıcı	37	17
S11 - Aşağıdaki cihazlardan hangileri siber saldırılara maruz kalabilir?	Kablosuz bebek monitörü	61,1	42,4
	IP kamera	77,7	67,3
	Akıllı TV	74	72,5
	Akıllı buzdolabı	53,7	41
	Yönlendirici (modem)	83,3	74,2
	Kablosuz yazıcı	57,4	42,4

Bilgi sahibi katılımcılar ile diğer katılımcıların satın alınan cihazlardaki varsayılan parolaları ilk kurulumda değiştirme oranları arasında istatistiksel açıdan anlamlı fark bulunduğu görülmüştür. Bilgi sahibi kişilerin satın aldıkları modem, IP kamera gibi cihazlarla birlikte verilen varsayılan parolayı ilk kurulumda değiştirme oranı %72 iken, diğer katılımcılarda bu oran %57,5'dir.

Güvenli parola seçim sorusunda bilgi sahibi katılımcılar ile diğer katılımcıların "7ujMko0admin" ve "SEays214." seçeneklerini tercih etme oranlarında istatistiksel açıdan anlamlı bir farklılık tespit edilmemiştir.

Bilgi sahibi katılımcılar ve diğer katılımcıların parola saklama tercihlerinin dağılımında istatistiksel açıdan anlamlı fark olduğu görülmüş olup, bilgi sahibi katılımcıların parolalarını akılda tutma oranı %58,5, diğer katılımcıların parolalarını akılda tutma oranı %71,3'tür. Bilgi sahibi katılımcıların parola yönetim programı kullanma oranı %17, diğer katılımcıların parola yönetim programı kullanma oranı %4'tür.

Parola seçimi konusunda bilgi sahibi katılımcıların her hesap için ayrı parola seçme oranının diğer katılımcılara oranla daha yüksek olduğu ancak yanıtların genel dağılımı dikkate alındığında tercihler arasında istatistiksel açıdan anlamlı bir fark bulunmadığı görülmüştür.

Bir siber saldırının hedefi olma ihtimaline dair her iki katılımcı grubun verdikleri yanıtlar arasında istatistiksel açıdan anlamlı fark bulunduğu tespit edilmiştir. Bilgi sahibi katılımcılardan kendilerini bir siber saldırının hedefi olma ihtimalini çok yüksek ve kesin olarak değerlendirenlerin oranı %24,1 iken diğer katılımcılarda bu oran %8,2'dir. Ki-Kare testine tabi tutulan yanıtlara yönelik istatistiksel analiz sonuçları Çizelge-6'da sunulmuştur.

6. Tartışma

Katılımcıların parola seçerken zor tahmin edilen ve akılda kalıcılığı bulunan parolaları tercih etmesi bireylerde belirli bir güvenli parola seçim kriterinin oluştuğunu göstermektedir. Katılımcılar yeni bir parola belirlerken kullandıkları birkaç parola içerisinden seçim yapmakta ve parolalarını diğer saklama yöntemlerine nazaran akılda tutmayı tercih etmektedir. Katılımcılar evlerindeki yönlendiricinin yönetici parolasını bankacılık, e-posta ve sosyal medya hesap parolalarından daha önemsiz görmektedir.

Katılımcılar karakter sayısı fazla ve farklı öz nitelikli karakterlerden oluşan parolaların güvenli olduğunu bilmektedir. Ancak üç yıldır çeşitli siber saldırılarda rolü olan Mirai zararlı yazılımının kaynak kodlarında kırılacak parolalar arasında bulunan ve Dahua marka bir kısım IP kameraların varsayılan parolası olduğu bilinen "7ujMko0admin" seçeneğinin katılımcıların çoğunluğu tarafından en güvenli parola olarak tercih edilmesi katılımcıların Mirai tarafından hedef alınan parola kütüphanesini bilmediğini göstermektedir.

Katılımcılar çoğunlukla satın aldıkları bir cihazın varsayılan parolasını ilk kurulumda değiştirmektedir ancak her beş katılımcıdan ikisinin satın aldıkları cihazlardaki varsayılan parolayı ilk kurulumda değiştirmemesi bu konuda ciddi bir bilinçsizlik olduğunu göstermektedir. Katılımcılarda internete bağlı nesnelerin siber saldırıya maruz kalabileceği bilinci kısmen oluşsa da bu nesnelerle siber saldırı yapılabileceği bilinci yeterli seviyede değildir.

Katılımcıların çoğunluğu bir siber saldırıya hedef olma ihtimalinin bulunmadığını veya bu ihtimalin az olduğunu belirtmiştir. İsteğe bağlı beyan edilen görüş ve önerilerin toplandığı son soruya bir kısım katılımcılar "bir siber saldırının hedefi olmak için istihbarat, emniyet vb. kritik bir birimde çalışıyor olmak gerektiği" ve "sıradan kullanıcıların siber saldırıya hedef olmasının mümkün olmadığı" içerikli yanıtlar vermiştir. Her iki durum birlikte değerlendirildiğinde, katılımcıların sıradan kullanıcıların bir siber saldırıya hedef olmayacağına

Çizelge-6: Bilgi Teknolojileri ve Siber Güvenlik Alanında Eğitim / İş Durumu Değişkenine Göre Yanıtların Ki-Kare Testi Sonuçları

Soru		Bilgi sahibi katılımcı mı? Evet (%)	Hayır (%)	χ 2	sd	p
S4 - Satın aldığım modem, IP kamera vb. cihazlarla birlikte gelen admin, root vb. parolayı ilk kurulumda değiştiririm. (Yanıtlar kategorik olarak yeniden düzenlenmiştir)	Evet	72,2	57,5	4,207	1	0,04
	Hayır	27,8	42,5			
S6 - Bir siber saldırının hedefi olma ihtimalinizi 1-5 arasında puanlayınız. (5 en yüksek ihtimal)	1. Hedef olma ihtimalim yoktur.	13	17,3	16,14	4	0,003
	2. Hedef olma ihtimalim azdır.	31,5	47,6			
	3. Hedef olup olmama ihtimalim aynıdır.	31,5	26,9			
	4. Hedef olma ihtimalim yüksektir.	9,3	4,2			
	5. Kesinlikle hedefim.	14,8	4			
S13 - Sizce aşağıdakilerden hangisi en güvenli paroladır?	7ujMko0admin	48,1	47,5	0,42	1	0,838
	SEays214.	44,4	46,7			
	Hepsi aynı paroladır.	7,4	6,5			
S14 - Parolalarınızı nasıl seçersiniz?	Kullandığım birkaç parolam var onların arasından seçerim.	51,9	67,1	5,289	3	0,152
	Çoğunlukla ayrı parolalar seçerim, nadiren bunlar birbirinin aynı olabilir.	14,8	10,5			
	Her hesap için ayrı parola seçerim.	25,9	15,9			
S15 - Parolalarınızı çoğunlukla nasıl saklamayı tercih edersiniz?	Kâğıda, post-it'e vb. fiziksel bir ortama yazarım.	9,4	6,8	14,32	4	0,006
	Bilgisayarımda / cep telefonumda bir dosya üzerine kaydederim.	11,3	12,5			
	Web tarayıcıma hatırlaması için kaydederim.	3,8	5,1			
	Aklımda tutarım.	58,5	71,3			
	Parola yönetim programı kullanırım ve ona kaydederim.	17	4,3			

dair algılarının bulunduğu sonucuna varılmıştır. İleri düzey kalıcı tehdit saldırıları (advance persistent threat - APT) söz konusu olduğunda bu algı kabul edilebilir olsa dahi nesnelerin internetini etkileyen zararlı yazılımlar açısından ele alındığında bu algının geçerli olmadığı değerlendirilmektedir.

Bilgi teknolojileri veya siber güvelik alanında eğitim alan yahut çalışan kişiler diğer katılımcılara kıyasla nesnelerin internetinin güvenliği konusunda daha bilinçli ve temkinlidir ancak bu kişilerce "7ujMko0admin" seçeneğinin güvenli parola olarak seçilmiş olması Mirai zararlı yazılımı tarafından hedef alınan parola kütüphanesinin yeterince bilinmediğini göstermektedir.

Katılımcıların çoğunluğu bilgisayarlarında işletim sistemi olarak Windows dağıtımlarını, web tarayıcı olarak Google Chrome uygulamasını tercih etmektedir. Ağa bağlı nesnelerin varsayılan parolalar veya kolay parolalar ile kullanımını engelleyecek çözümlerin tasarımında bu çalışmada tespit edilen tercih ve eğilimlerin göz önünde bulundurulması söz konusu çözümlerin erişilebilirliğini, kullanılabilirliğini ve etkinliğini arttıracaktır.

7. Sonuç

Mirai zararlı yazılımı uzun bir süredir güvenlik uzmanları tarafından bilinmektedir. Güvenlik

uzmanları tarafından nesnelerin interneti cihazlarında varsayılan oturum açma bilgilerinin kullanımının sona erdiği yanılgısına kapılabilir. Ancak bu araştırma göstermiştir ki halen ülkemizdeki her beş kullanıcıdan ikisi cihazlarının ilk kurulumunda varsayılan parolayı değiştirmemektedir. Uzmanlar tarafından yapılan araştırmalar neticesinde elde edilen bilgilerin uç kullanıcılara, bu kullanıcıların anlayacağı seviyede aktarımı ve kullanıcılardaki farkındalık seviyesinin arzu edilen düzeye çıkarılması hususunda eksiklikler bulunduğu açıktır. Bu eksikliklerin hızlı ve geçici yöntemlerle giderilmesini beklemek gerçekçi bir yaklaşım olmayacaktır. Ülkemizde ilköğretim çağından itibaren bireylere temel bilişim eğitimi verilmekte, kamu kurumları ve özel sektörde çalışanlara bilgi güvenliği farkındalık eğitimleri verilmektedir. Ulusal siber güvenlik eylem planına eklenecek hususlar ve ortaya konacak bir irade ile ilköğretimden itibaren bilgi güvenliği farkındalık eğitimleri verilmeli ve nesnelerin internetinin güvenliği konusu bu eğitim kapsamında ele alınmalıdır.

Nesnelerin interneti cihazlarının tasarımından kaynaklanan zafiyetlerin önlenmesi konusunda standartlar ve belgelendirme süreçleri büyük rol oynamaktadır.

İnternete bağlı nesnelerin güvenlik alanında test ve sertifikasyonun sağlanması amacıyla yedi ayrı değerlendirme seviyesinden oluşan ISO/IEC 15408 Ortak Kriterler Belgelendirmesi sürecinden faydalanılması yaygın bir uygulama olsa dahi bu sürecin uzunluğu, harcanan efor ve maliyetlerin üreticilere getirdiği yük eleştirilmektedir [34]. Akıllı bir televizyonun ISO/IEC 15408 Ortak Kriterler Belgelendirmesi kapsamında önceden belirlenmiş güvenlik kriterlerine uygunluğunun ikinci derece değerlendirme seviyesinde (EAL2) test edilmesi dört ay sürmüştür [35]. ISO/IEC 15408 Ortak Kriterler Belgelendirmesi sürecinin ikinci derece değerlendirme seviyesinin (EAL2) milli karşılığı olarak Türk Standartları Enstitüsü tarafından geliştirilen TSEK 505 Temel Seviye Belgelendirmesi sürecinde daha az maliyetle ve daha kısa sürede bilişim teknolojileri ürünlerinin test ve belgelendirmesinin tamamlanacağı öngörülmektedir [36]. ABD ve İngiltere'deki yasal düzenlemelerin ülkemize de uyarlanarak ülkemiz pazarına arz edilen ağ erişim yetenekli nesnelerin her bir nesne için farklı varsayılan parola ile satışının zorunlu hale getirilmesi ve bu nesnelerin ETSI TS 103 645 "Cyber Security for Consumer Internet of Things" tarafından tespit edilen güvenlik kriterleri dikkate alınarak TSEK 505 Temel Seviye Güvenlik Belgelendirmesi sürecine tabi tutulması ülkemiz dahilindeki nesnelerin interneti ekosisteminin güvenliğini arttıracaktır.

Kaynakça

[1] A. Dulaunoy, G. Wagener, and S. Mokaddem, "An extended analysis of an IoT malware from a blackhole network," in *TNC17 Networking Conference*, Linz, Austria, 2017, p. 42.

[2] "Internet of things at a glance," *Cisco*, 2016. [Online]. Available: https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf. [Accessed: 06-May-2019].

[3] "OWASP Internet of Things Project," *OWASP*. [Online]. Available: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project #tab=IoT_Top_10. [Accessed: 03-May-2019].

[4] R. Hallman, J. Bryan, G. Palavicini, J. Divita, and J. Romero-Mariona, "IoDDoS - The Internet of distributed denial of sevice attacks - a case study of the Mirai malware and IoT-based botnets," in *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security*, Porto, Portugal, 2017, pp. 47–58.

[5] J. Margolis, T. T. Oh, S. Jadhav, Y. H. Kim and J. N. Kim, "An In-Depth Analysis of the Mirai Botnet," *2017 International Conference on Software Security and Assurance (ICSSA)*, Altoona, PA, USA, 2017, pp. 6-12.

[6] S. Hilton, "Dyn analysis summary of friday October 21 attack," *Dyn Blog*, 26-Oct-2016. [Online]. Available: https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/. [Accessed: 05-May-2019].

[7] "jgamblin/Mirai-Source-Code," *GitHub*, 25-Oct-2016. [Online]. Available:https://github.com/jgamblin/MiraiSourceCode/tree/master/mirai. [Accessed: 01-May-2019].

[8] I. Zeifman, B. Herzberg, D. Bekerman, "Breaking down mirai: an IoT DDoS botnet analysis," *Imperva*, 26-Oct-2016. [Online]. Available: https://www.imperva.com/blog/malwareanalysis-mirai-ddos-botnet.html. [Accessed: 07-May-2019].

[9] Y. Xu, H. Koide, D. V. Vargas and K. Sakurai, "Tracing Mirai malware in networked system," in *2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW)*, Takayama, Japan, 2018, pp. 534-538.

[10] H. Sinanović and S. Mrdovic, "Analysis of Mirai malicious software," in *2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, Split, 2017, pp. 1-5.

[11] T. S. Gopal, M. Meerolla, G. Jyostna, P. Reddy Lakshmi Eswari and E. Magesh, "Mitigating Mirai malware spreading in IoT environment," in *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Bangalore, Karnataka, India, 2018, pp. 2226-2230.

[12] L. Labrovic, "The new Okiru mirai botnet, spectre is slowing down ecommerce websites and more in this weeks news," *GlobalDots*, 19-Jan-2018. [Online]. Available: https://www.globaldots .com/new-okiru-mirai-botnet-spectre-slowing-ecommerce-websites-weeks-news/. [Accessed: 08-May-2019].

[13] G. Kambourakis, C. Kolias and A. Stavrou, "The Mirai botnet and the IoT zombie armies," in *MILCOM 2017 - 2017 IEEE Military Communications Conference*, Baltimore, MD, USA, 2017, pp. 267-272.

[14] "Hacker creates seven new variants of the Mirai botnet," *AvastBlog*, 25-Oct-2018. [Online]. Available: https://blog.avast.com/hacker-creates-seven-new-variants-of-the-mirai-botnet. [Accessed: 06-May-2019].

[15] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[16] Y. Ji, L. Yao, S. Liu, H. Yao, Q. Ye and R. Wang, "The study on the botnet and its prevention policies in the internet of things," in *2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, Nanjing, 2018, pp. 837-842.

[17] M. Antonakakis et al. "Understanding the mirai botnet", in Proceedings of the 26th USENIX Conference on Security Symposium, 2017, Vancouver, BC, Canada; pp. 1093-1110.

[18] "Nokia threat intelligence report – 2019," [Online]. Available: https://onestore.nokia.com/asset/205835?did=d000000016z&utm_campaign=threatintelligence18&utm_source=marketo&utm_medium=LandingPage&utm_content=report&utm_term=awareness. [Accessed: 02-May-2019].

[19] R. Nigam, "New Mirai variant targets enterprise wireless presentation & display systems," *Unit42*, 01-Apr-2019. [Online]. Available: https://unit42.paloaltonetworks.com/new-mirai-variant-targets-enterprise-wireless-presentation-display-systems/. [Accessed: 06-May-2019].

[20] K. W. Chang, "Mirai is still alive and using multiple old exploits on home routers," *Ixia*. 15-Apr-2019. [Online]. Available: https://www.ixiacom.com/company/blog/mirai-still-alive-and-using-multiple-old-exploits-home-routers. [Accessed: 03-May-2019].

[21] M.S.Tok, "Nesnelerin İnternetinde Botnetler", Yüksek Lisans Tezi, TOBB Ekonomi ve Teknoloji Üniversitesi, Ağustos 2019.

[22] USCERT, "Heightened ddos threat posed by Mirai and other botnets", *Alert TA16-288A*, 14-Oct-2016 (revised 30-Oct-2017). [Online]. Available: www.us-cert.gov/ncas/alerts/TA16-288A. [Accessed: 02-May-2019].

[23] "SB-327 Information privacy: connected devices", *Senate Bill No.327*, 28-Sep-2018. [Online]. Available: https://leginfo. legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327. [Accessed: 05-May-2019].

[24] "Code of practice for consumer IOT security," *Secure by Design*, 28-Feb-2019. [Online]. Available: https://www.gov.uk/government/publications/secure-by-design/code-of-practice-for-consumer-iot-security. [Accessed: 06-May-2019].

[25] ETSI TS 103 645 (2019). *CYBER; Cyber Security for Consumer Internet of Things,* European Telecommunications Standards Institute, Sophia-Antipolis, France.

[26] "Our Increasingly Connected Lives: Survey conducted by ESET in collaboration with the National Cyber Security Alliance," 24-Oct-2016. [Online]. Available: https://cdn3.esetstatic.com/eset/US/resources/press/ESET_ConnectedLives-DataSummary.pdf. [Accessed: 01-May-2019].

[27] M. Ghiglieri, M. Volkamer, and K. Renaud, "Exploring consumers' attitudes of smart tv related privacy risks," in *International Conference on Human Aspects of Information Security, Privacy and Trust Lecture Notes in Computer Science (HAS 2017)*, Vancouver, Canada, 2017, pp. 656–674.

[28] C. Mcdermott, J. Isaacs, and A. Petrovski, "Evaluating awareness and perception of botnet activity within consumer internet-of-things (IoT) networks," *Informatics,* vol. 6, no. 1, p. 8, 2019.

[29] T. Talan, C. Aktürk, A. Korkmaz, S. Gülseçen, "Üniversite öğrencilerinin akıllı telefon kullanımında güvenlik farkındalığı," *Istanbul Journal of Open and Distance Education*, vol. 1, no. 2, pp. 61-75, 2016.

[30] Ö.E. Akgün, M. Topal, “Eğitim fakültesi son sınıf öğrencilerinin bilişim güvenliği farkındalıkları: Sakarya Üniversitesi Eğitim Fakültesi örneği,” *Sakarya Üniversitesi Eğitim Fakültesi Dergisi*, vol. 5, no. 2, pp. 98-121, 2015.

[31] M. Tekerek, A Tekerek, “Öğrencilerin bilgi güvenliği farkındalığı üzerine bir araştırma”, *Turkish Journal of Education*, vol. 2, no. 3, pp. 61-70, 2013.

[32] “Digital in 2018 in Western Asia Part 1 - North-West”, 29-Jan-2018. [Online]. Available: https://www.slideshare.net/wearesocial/digital-in-2018-in-western-asia-part-1-northwest-86865983. [Accessed: 07-May-2019].

[33] A. Houston, *The survey handbook*, Washington, DC: Department of the Navy Total Quality Leadership Office, 1997. [Online]. Available: http://unpan1.un.org/intradoc/groups/public/documents /aspa/unpan002507.pdf [Accessed: 01-May-2019].

[34] G. Baldini, A. Skarmeta, E. Fourneret, R. Neisse, B. Legeard and F. Le Gall, "Security certification and labelling in internet of things," in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, Reston, VA, 2016, pp. 627-632.

[35] S. Kang and S. Kim, “How to obtain common criteria certification of smart TV for home IoT security and reliability,” *Symmetry*, vol. 9, no. 10, p. 233, 2017.

[36] “Temel seviye güvenlik belgelendirmesi”, *TSE*. [Online]. Available: https://www.tse.org.tr/IcerikDetay?ID=2061&ParentID=3312. [Accessed: 02-May-2019].