İşletme Akademisi Dergisi
2021, 2 (2): 208-219
DOI:10.26677/TR1010.2021.787
Dergi web sayfası: www.isakder.org

Derleme Makalesi

İşletmelerin Kâbusu: İş E-Postası Dolandırıcılığı (BEC)

Dr. Öğr. Üyesi Murat ERDOĞAN

Akdeniz Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, İşletme ABD, Antalya, Türkiye.
muraterdogan@akdeniz.edu.tr, https://orcid.org/0000-0002-4506-0731

Öz

Siber dolandırıcılar son zamanlarda işletmeleri ve çalışanlarını hedef alarak önemli zararlarla karşı karşıya bırakmaktadır. Siber dolandırıcılık kuruluşlara ciddi zararlar vermekte ve bu suçlar kısa sürede de tespit edilememektedir. Son yıllarda yapılan çalışmalarda bir siber ihlalin tespit edilebilmesinin ortalama 206 gün sürdüğü, kötü amaçlı yazılımların %95'inin e-posta yoluyla gönderildiği, işletmelerin %60'ından fazlasının kimlik avı ve sosyal mühendislik saldırılarına maruz kaldığı ve yüksek tutarlarda iş e-postası dolandırıcılık (BEC) kaybı yaşandığı tespit edilmiştir. BEC, bir kuruluşun kritik önem seviyesindeki bilgilerine erişilmesi, e-posta tabanlı bir dolandırıcılık yöntemi ile tasarlanan ve sonucunda da maddi bir kazanç sağlanan zararlı bir kimlik avı biçimi olarak tanımlanmaktadır. Bu çalışmada, ana hedefi işletmeler olan ve dolandırıcılık yöntemlerinden birisi durumundaki BEC dolandırıcılığı üzerine odaklanılarak sistemin nasıl işlediği, hangi yöntemlerin kullanıldığı kapsamlı bir şekilde ele alınarak örnek olaylara yer verilmiştir. Örnek olaylar incelendiğinde, failler herhangi bir olağanüstü çabaya gerek duymadan bazen bir yapay zekâ tabanlı bir yazılım kullanma yoluyla işletme yöneticisi veya çalışanı gibi davranarak hileli bir işlemi kolaylıkla gerçekleştirebildiği görülmektedir.

Anahtar Kelimeler: Siber Dolandırıcılık, CEO Dolandırıcılığı, İş e-postası Dolandırıcılığı (BEC)

Makale Gönderme Tarihi: 20.05.2021

Makale Kabul tarihi: 23.06.2021

Önerilen Atıf:

Erdoğan, M. (2021). İşletmelerin Kâbusu: İş E-Postası Dolandırıcılığı (BEC), *İşletme Akademisi Dergisi,* 2 (2): 208-219.

Journal of Business Academy
2021, 2 (2): 208-219.
DOI:10.26677/TR1010.2021.786
Web pages: www.isakder.org

Review Article

Business Nightmare: Business E-Mail Compromise (BEC)

Dr. Murat ERDOĞAN

Akdeniz University, Faculty of Economic and Administrative Sciences, Antalya, Turkey.
muraterdogan@akdeniz.edu.tr, https://orcid.org/0000-0002-4506-0731

Abstract

Cyber fraudsters have recently targeted businesses and their employees, leaving them with significant losses. Cyber fraud causes serious damage to organizations and these crimes cannot be detected in a short time. In recent years, it takes an average of 206 days to detect a cyber breach, 95% of malware is sent via email, more than 60% of businesses are exposed to phishing and social engineering attacks, and high amounts of business email fraud (BEC) loss was detected. BEC is defined as a malicious form of phishing designed with an email-based fraud method to access critical information of an organization, resulting in financial gain. This study focuses on BEC fraud, which is one of the cyber attack and fraud methods and the main target of businesses, and includes case studies by comprehensively discussing how the system works and which methods are used. When the case studies are examined, it is seen that the perpetrators can easily perform a fraudulent transaction by pretending to be a business manager or employee, sometimes by using an artificial intelligence-based software, without the need for any extraordinary effort.

Keywords: Cyber Fraud,, CEO Fraud, Business e-mail Compromise (BEC)

Received: 20.05.2021

Accepted: 23.06.2021

Suggested Citation:

Erdoğan, M. (2021). Business Nightmare: Business E-Mail Compromise (BEC), *Journal of Business Academy*, 2 (2): 208-219.

1.GİRİŞ

Cybersecurity Ventures tarafından yapılan bir araştırmaya göre siber suç maliyetinin yılda 6 trilyon dolara mal olacağı diğer taraftan Gartner tarafından yapılan araştırmaya göre kuruluşların siber tehditlere karşı savunmalarını geliştirmesinden ve kendi şirketleri de dâhil olmak üzere bu tür tehditlerdeki artıştan dolayı küresel bilgi güvenliği pazarının 2022 yılında 170,4 milyar dolara ulaşılacağı öngörülmüştür (Sobers, 2021). Bu istatistikler siber suçların ve bu kapsamda gerçekleştirilen dolandırıcılıkların sadece bir işletmenin bütünlüğüne veya insanların bilgilerine yönelik bir tehdit değil aynı zamanda ekonomik bir tehdit olarak da ciddiye alınması gerektiğini göstermektedir (Cybint, 2020). Dolandırıcılar eylemlerini her geçen gün farklılaştırıp detaylandırmaktadır. Örneğin BEC dolandırıcılığı genel müdürlerin veya finans müdürlerinin e-posta hesaplarının hacklenmesi veya sızdırılmasıyla elektronik ödemelerin sahte konumlara gönderilmesini talep eden sahte e-postalar gönderilmesi şeklinde rutin bir hal almasının ardından izleyen yıllarda kişisel e-postaların ele geçirilmesi, satıcı e-postalarının ele geçirilmesi, sahte avukat e-postalarının türetilmesi, vergi bildirim formlarının düzenlenmesi vb. gibi farklı yöntemler kullanılmaya başlanmıştır (FBI, 2020).

İş e-postası dolandırıcılığı (BEC), dünyanın her yerindeki her sektörden her büyüklükteki kuruluşu hedefleyen büyük ve büyüyen bir sorun olup kuruluşları milyarlarca dolarlık potansiyel kayıplara maruz bırakmıştır. Örneğin dünyanın en büyük teknoloji şirketlerinden olan Google ve Facebook "Rimasauskas" adlı bir şirketin kendilerine sahte faturalar göndermesi sonucunda 100 milyon doların üzerinde bir kimlik avı dolandırıcılığına maruz kalmıştır (Gibbs, 2017).

Bu tür saldırılarda siber suçlular, çalışanları banka havalesi yapmak, yeni olduğu iddia edilen bir proje için ödeme yapmak veya gizli bilgileri sağlamak gibi belirli bir eylemi gerçekleştirmeleri için kandırmayı ve ikna etmeyi amaçlar. Bu saldırılarda bilgisayar korsanları, kurumsal e-posta hesaplarını suiistimal ederek yasal hesaplarla neredeyse aynı olan yeni hesaplar oluşturur. Ardından saldırganlar, e-posta hesaplarının sahiplerinin kimliğine bürünür ve kurbanlara mesaj gönderir. Suçlular genellikle CEO ve CFO gibi üst düzey yöneticileri veya diğer kademelerdeki yöneticileri taklit eder. Bu nedenle, e-posta alışverişi yoluyla güven bağı kurulduğunda, dolandırıcı hedeften gizli bilgileri paylaşmasını, sahte bir banka hesabına para transfer etmesini veya fidye yazılımı veya başka kötü amaçlı yazılım içeren kötü amaçlı bir dosyaya tıklamasını ister. BEC saldırıları, CEO dolandırıcılığı veya E-postadaki Adam dolandırıcılığı olarak da bilinir (Gatefy, 2021).

2. İŞ E-POSTASI DOLANDIRICILIĞI (BEC) ve EN YAYGIN BEŞ UYGULANMA BİÇİMİ

BEC ve/veya e-posta hesabı dolandırıcılığı (EAC) diğer bilinen adıyla Ceo Fraud, hem işletmeleri hem de banka havalesi ödemeleri yapan bireyleri hedef alan karmaşık bir dolandırıcılık türüdür. BEC, hesap numaralarını, erişim kodlarını veya diğer hassas bilgileri elde etmek amacıyla şirket personeline sahte veya dolandırıcılık amaçlı e-postaların yönlendirildiği hedefli kimlik avı uygulamasının bir çeşidi olarak tanımlanabilir (Zweighaft, 2017). Diğer bir ifade ile BEC dolandırıcılığı, siber saldırganın üst düzey bir yöneticiyi (CIO, CEO, CFO, vb.) taklit ettiği ve bir çalışanın veya müşterinin para ve/veya hassas verileri aktarmasını sağlamaya çalıştığı bir tür kimlik avı planıdır. BEC, yabancı tedarikçilerle çalışan işletmeleri (bireyleri değil) ve/veya düzenli olarak banka havalesi ödemeleri yapan işletmeleri hedef alan bir dolandırıcılıktır. EAC ise daha çok bireyleri hedef alan bir dolandırıcılık yöntemidir. Bu karmaşık dolandırıcılıklar, yetkisiz para transferi yapmak için sosyal mühendislik veya bilgisayar izinsiz giriş teknikleri

aracılığıyla e-posta hesaplarını suiistimal eden dolandırıcılar tarafından gerçekleştirilmektedir. Bu tür bir dolandırıcılık, çoğu zaman bir kişi, yetkisiz fon transferleri gerçekleştirmek için sosyal mühendislik veya bilgisayar izinsiz giriş teknikleri yoluyla meşru iş e-posta hesaplarını manipüle eder (FBI, 2018) sonucunda da işletmeler önemli kayıplar yaşar. 2020 yılında Federal Soruşturma Bürosu (FBI) tarafından yayınlanan *"Internet Suç Raporu"* başlıklı çalışmada iş e-postası dolandırıcılığı ve çalışan kimliğine bürünme şeklinde gerçekleşen dolandırıcılık yönteminin en maliyetli siber güvenlik tehditlerinden biri olduğu ve 1.8 milyar doların üzerinde bir kayba neden olduğu ifade edilmiştir (FBI, 2020).

BEC dolandırıcılığı çeşitli yöntemler üzerinden kurgulanmaktadır. Aşağıda belirtilen Tablo 1'de FBI tarafından yapılan araştırmalarda en yaygın kullanılan türlere yer verilmiştir.

Tablo 1. BEC Dolandırıcılığının En Yaygın Türleri

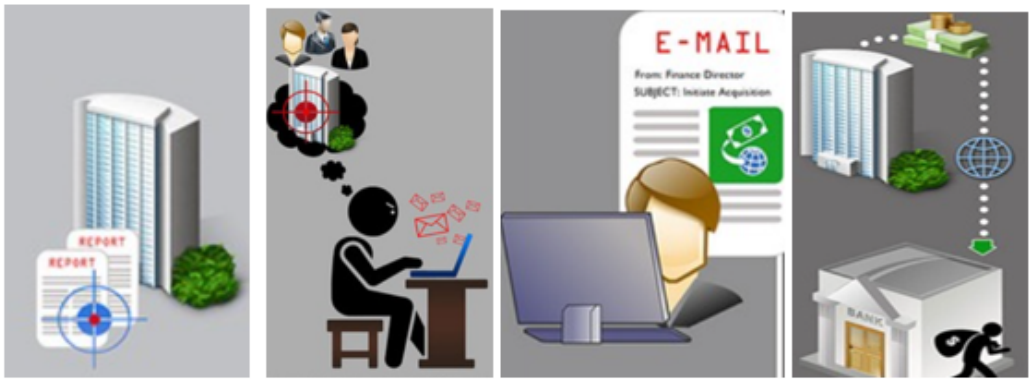
CEO Dolandırıcılığı	Saldırganlar, bir şirketin CEO'sunu veya yöneticisini taklit eder. CEO olarak, muhasebe veya finans departmanındaki bir çalışanın saldırgan tarafından kontrol edilen bir hesaba para transfer etmesini isterler.
Sahte Fatura Düzeni	Yabancı tedarikçileri olan şirketler genellikle bu taktikle hedef alınır; burada saldırganlar, dolandırıcıların sahip olduğu bir hesaba ödemeler için para transferi talep eden tedarikçiler gibi davranırlar.
E-posta Hesabı Ele Geçirme Saldırısı	Bir yöneticinin veya çalışanın e-posta hesabı saldırıya uğrar ve e-posta bağlantılarında listelenen satıcılara fatura ödemeleri talep etmek için kullanılır. Ödemeler daha sonra sahte banka hesaplarına gönderilir.
Avukat Kimliğine Bürünme	Saldırganlar, hassas konulardan sorumlu hukuk firmasının bir avukatını veya başka bir temsilcisini taklit eder. Bu tür saldırılar genellikle iş gününün sonunda, mağdurların iletişimin geçerliliğini sorgulayacak bilgi veya yetkiye sahip olmayan düşük seviyeli çalışanlar olduğu durumlarda e-posta veya telefon yoluyla gerçekleşir.
Veri Hırsızlığı	İnsan kaynakları ve muhasebe çalışanları, çalışanlar veya yöneticiler hakkında kişisel veya diğer hassas bilgileri elde etmek için hedef alınır. Bu veriler gelecekteki saldırıların başarılı olabilmesi için dolandırıcıya çok önemli avantaj sağlar.

Kaynak: FBI, 2017.

3. BEC DOLANDIRICILIKLARI NASIL ÇALIŞIR?

Bu tür bir dolandırıcılıkta dolandırıcı, hedef işletme hakkında detaylı bilgi toplar. Bazen dolandırıcı bu bilgilere ulaşmak için aylarca veri toplayabilir. Örneğin hedef şirket ile ticari ilişkisi olan bir diğer şirket arasındaki yazışmalar dolandırıcılar tarafından izlenmeye başlar. İki şirket arasındaki ticari yazışmaların takip edilmesi sonucunda olası bir satın alma veya para transferi işlemlerinin gerçekleştirileceği sırada dolandırıcılar hemen harekete geçer. Yeterli veriye sahip olduktan sonra hedef işletmedeki yüksek rütbeli bir kişi gibi davranarak aramalar veya e-postalar gönderir. Söz konusu görüşmede acil ödeme talebinde bulunulur buna ek olarak *"Şirket*

size güveniyor", *"Şu anda müsait değilim"* gibi bir dil kullanılır ve çalışanın normal yetkilendirme prosedürlerine uymaması rica olunur. Ardından sürecin nasıl devam edileceğine ilişkin talimatlar daha sonra da üçüncü bir kişi tarafından veya e-posta yoluyla verilebilir. İlgili e-postada genellikle hassas bir duruma vergi kontrolü, işletme birleşmesi, satın alma vb. gibi atıfta bulunulur. Genellikle yapılan talep, Avrupa dışındaki bankalara yapılan uluslararası ödemeler içindir. Bu süreç sonucunda hedef çalışan, parayı dolandırıcı tarafından kontrol edilen bir hesaba aktarır (European Banking Federation). Söz konusu işleyişe özet olarak Şekil 1'de yer verilmiştir.



Aşama 1

Dolandırıcılar, hedef bir işletmeyi belirler ve şirketin ve yöneticilerinin profilini çıkarmak için halka açık çevrimiçi bilgileri kullanır.

Aşama 2

Dolandırıcılar, şirket yetkililerini hedef alan karmaşık hedef odaklı kimlik avı e-postaları gönderir veya telefon görüşmeleri yapar. Bilgisayar korsanları genellikle meşru bir e-posta hesabını (genellikle CEO veya finans departmanındaki biri) ihlal etmeye çalışır.

Aşama 3

Hedef çalışanın güveninin kazanılması veya inandırılması sonrasında onları veya şirketin iş ortaklarını para havale etmek veya hesaplarına çek göndermek için kandırır.

Aşama 4

Fonlar, suç örgütü tarafından kontrol edilen bir banka hesabına yönlendirilir ve ardından izlenmesi neredeyse imkânsız olan diğer hesaplara hızlı bir şekilde dağıtılır.

Şekil 1. BEC Dolandırıcılık Aşamaları (**Kaynak:** FBI, 2017)

Japonya merkezli bir bilgisayar yazılım şirketi olan Trend Micro, 2016 yılında yayınlamış olduğu *"Milyar Dolarlık Dolandırıcılık: Kurumsal E-posta Dolandırıcılığı (BEC) Arkasındaki Rakamlar"* başlıklı çalışmasında şirketlerin finans departmanı çalışanlarının, BEC saldırılarının en çok hedef aldığı kişiler olduğu, söz konusu çalışanların diğer taraflara para transferi gibi görevlerden sorumlu kişiler olduğu düşünüldüğünde dolandırıcılar için neden bu kişilerin hedef alındığının makul bir

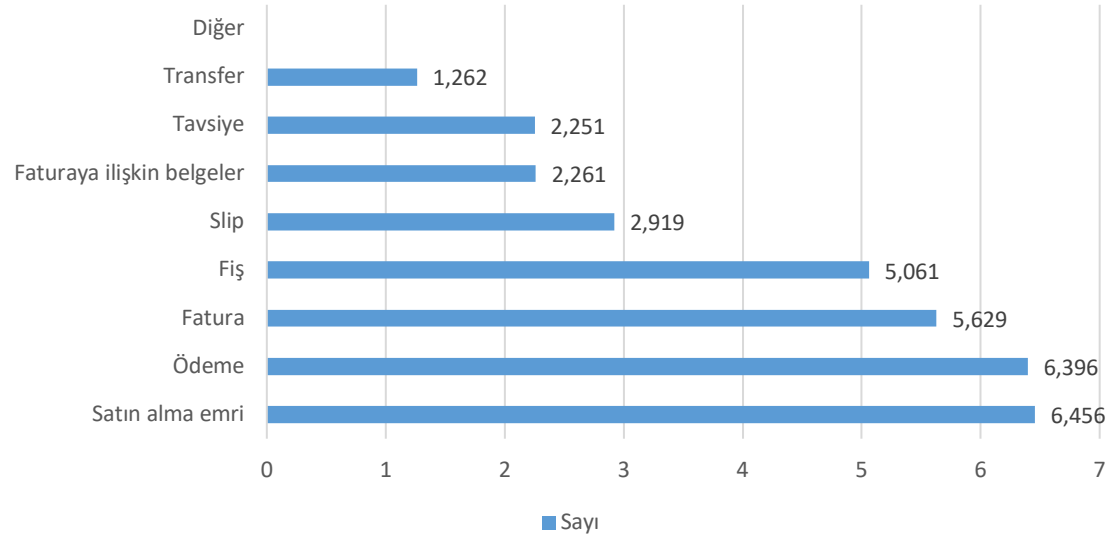
açıklaması olarak nitelendirilebilir. Diğer taraftan dolandırıcıların kendilerini en çok CEO izlenimi vererek saldırıda bulundukları görülmektedir. Dolandırıcıların en çok hedeflediği şirket pozisyonları ve çalışıyor izlenimi verdikleri pozisyonlar Tablo 2'de yer almaktadır.

Tablo 2. Hedeflenen Şirket Pozisyonları ve Dolandırıcıların Çalışıyor İzlenimi Verdikleri Pozisyonlar

Hedeflenen Şirket Pozisyonları	**%**
CFO	40,38
Finans Direktörü	9,62
Mali Kontrolör	5,77
Mali Müşavir	3,85
Finans Müdürü	3,85
Diğer	36,53
Dolandırıcıların Çalışıyor İzlenimi Verdikleri Pozisyonlar	**%**
CEO	31
Şirket Sahibi	17
Genel Müdür	15
Şirket Sahibi ve CEO	13
Üst Yönetici	4
Diğer	20

Yine aynı şirketin 2018 yılında yayınlamış olduğu *"İş E-posta Dolandırıcılığı (BEC) Planlarındaki Trendleri İzleme"* raporunda BEC saldırılarının eklerinde kullanılan en popüler dosya adı kategorilerine Grafik 1'de yer verilmiştir.

Grafik 1. BEC Saldırılarının Eklerinde Kullanılan En popüler Dosya Adı Kategorileri



Kaynak: Trend Micro, 2018.

4.VAKALAR

Dünyanın her yerinde BEC dolandırıcılığına yönelik birçok vaka yaşanmaktadır. Bu başlık altında farklı ülkelerde yaşanmış olan BEC dolandırıcılığına ilişkin 5 farklı vakaya yer verilmiştir.

4.1 Vaka 1[1]

Amerika Birleşik Devletlerinde faaliyet gösteren bir şirketin muhasebecisi, kısa bir süre önce, ülke dışında tatilde olan genel müdüründen, gün sonuna kadar tamamlanması gereken bir satın alma için para transferi talep eden bir e-posta alır. Ek olarak ilgili e-postada şirketin CEO'su daha fazla ayrıntı sağlamak için bir avukatın muhasebeci ile iletişime geçeceği ifade edilir. Muhasebeci daha önceden de bu tarz para transferlerini içeren mailler aldığından dolayı herhangi bir şüphe duymaz. E-postanın ardından avukatla iletişime geçer ve ilgili yetki mektubunu kaydederek CEO'nun imzası dâhil şirketin mührü ve Çin'deki bir bankaya 737 bin dolardan fazla havale yapma talimatlarını izler. Ertesi gün, CEO başka bir konuyla ilgili aradığında, muhasebeci banka havalesini bir gün önce tamamladığını söyler. CEO, e-postayı hiç göndermediğini ve iddia edilen satın alma hakkında hiçbir şey bilmediğini ifade eder. Şirket, bir e-posta dolandırıcılığının (BEC) kurbanı olur. Daha sonra ilgili soruşturma sürecinde ilgili e-postalar gözden geçirildiğinde önemli bir ipucu bulunur. CEO tarafından gönderilen e-postanın sonunda ".com" yerine ".co" yazıldığı, avukat tarafından sağlanan ekteki CEO'nun imzasınız sahte olduğu, şirket mührünün şirketin halka açık web sitesinden kesilip yapıştırıldığı ortaya çıkar. Diğer taraftan şirketin web sitesinde yer alan şirketin icra görevlilerinin ve e-posta adreslerinin ve bu kişilerin bir takvim yılı boyunca katılacağı etkinliklerin yer almasından dolayı dolandırıcıların bu bilgilerden yararlanarak eylemlerinde başarılı oldukları sonucuna varılır.[2]

4.2. Vaka 2[3]

Danimarka'da faaliyet gösteren GM Plast işletmesinin 2018 yılının nisan ayında şirket müdürünün e-posta adresi ele geçirilir. Şirket müdürü tarafından gönderilmiş gibi, 6 adet sahte fatura eşliğinde muhasebe departmanına bu faturalar gönderilir ve gereğinin yapılması istenir. İlgili maili alan çalışanlar toplamda 4 milyon 546 bin 555 doları farklı işletmelerin hesaplarına transfer ederler. Bu işletmelerden biri de Türkiye'de bulunan bir işletmedir ve söz konusu işletmeye 1 milyon 416 bin dolar transfer edilir. İlginç olanı söz konusu işletme 10 bin TL sermayeye sahiptir. İşletme kısa süre önce bir bankanın şubesinde hesap açtırmış ve o güne kadar herhangi bir ticari işlemde bulunmamıştır. Birkaç gün sonra bankanın ilgili şubesi telefonla aranarak ilgili hesaptaki paranın tamamının çekileceği bilgisini banka yetkililerine iletilir. İşletme hayali/paravan bir işletmedir, herhangi bir adresi yoktur ve kurucu olarak gösterilen kişi işçi statüsünde çalışan bir kişidir. Söz konusu parayı çekmek için gelen kişi 23 yaşında bir gençtir ve elindeki belgeler şüpheli olmasına rağmen ilgili banka yetkilileri 1 milyon 416 bin doları 23 yaşındaki gence teslim eder. Danimarkalı işletme olaydan haberdar olur olmaz yasal mercilere başvurur. Bakırköy Cumhuriyet Savcılığı harekete geçer. Önce hayali/paravan işletme yetkilileri yakalanır. Ardından asıl faillere ulaşılır. Failler Türkiye'de yerleşmiş olan Nijeryalı bilgisayar korsanlarıdır. Bilgisayarlarında yapılan incelemede 50'ye yakın dolandırıcılık bulgusuna ulaşılır. Dolandırıcılık soruşturması örgüt suçlamasına dönerken şüpheli sayısı yaklaşık olarak 100'dür. Kurban sayıları da her geçen gün artar. Bakırköy Cumhuriyet Savcılığı tarafından hazırlanan

[1] Bu örnek FBI'ın 2015 yılında yayınlamış olduğu "Business E-Mail Compromise: An Emerging Global Threat" başlıklı bilgilendirme metninden derlenmiştir (FBI, 2015).

[2] BEC dolandırıcılığı açısından, hem şirketler hem de bireyler hakkında kamuya açık bilgilerin mevcudiyeti, motive olmuş bir suçlu için çok sayıda potansiyel hedef sağlamaktadır (Cross ve Gillett, 2020).

[3] Bu örnek Barış Terkoğlu tarafından 30 Ocak 2020 tarihli Cumhuriyet Gazetesi'ndeki köşe yazısından alınmıştır (Terkoğlu, 2020).

iddianamelerde söz konusu sürecin sorumlularından biri de ilgili ödemeyi yapan banka olur. Özet olarak bankaya bu tutarda bir miktarın yalnızca İstanbul Ticaret Odası'ndan sorulması, parayı çekmeye gelen kişinin elindeki vekâletin sadece noterden teyit edildiğini, işletmenin adresinin fiilen araştırılmadığı ve 23 yaşındaki bir kişiye herhangi bir araştırma yapmadan ödenmesinin büyük bir ihmal olduğu ifade edilir.

4.3. Vaka 3[4]

Almanya merkezli bir şirketin CEO'sunun sesinin yapay zekâ ile taklit edilerek işletme 1.4 milyon dolar tutarında bir para kaybına uğrar. Olayda yapay zekâ tabanlı bir yazılım kullanılır. Siber dolandırıcılar herhangi bir ücret ödemeksizin herkesin erişimine açık bir yazılım kullanmaktadır. Mart ayında, İngiltere'de faaliyet gösteren bir enerji işletmesinin yöneticisi Almanya'daki patronundan bir telefon alır ve hiçbir şeyden şüphelenmez. Telefondaki ses, Macaristan'daki bir tedarikçiye acil olarak 243 bin dolar ödeme yapmasını talep eder. Oluşacak nakit açığının kısa sürede başka bir ödemeyle kapatılacağı ifade edilir fakat herhangi bir ödeme yapılmaz. Dolandırıcılar eylemlerine devam eder ve bu sefer yine Almanya'daki CEO gibi arayarak İngiltere'deki yöneticiden bir acil ödeme talep ederler. Olayda faillere ulaşılamaz.

Ses ile gerçekleştirilen dolandırıcılıklara karşı yazılım üreten bir işletme 2013 yılından günümüze ses taklidi ile gerçekleştirilen suçlarda %350 artış olduğunu ifade ettiler. Yapılan analizlerde bir işletmeye gelen her 638 telefon görüşmesinden birinde yapay olarak oluşturulan ses kullanıldığı belirtilmektedir. Yöneticilere ödeme gibi kritik talimatlarda telefon görüşmesinin ardından mutlaka e-posta vb. yazılı yöntemler kullanmaları gerektiğini vurgulanır.

4.4. Vaka 4[5]

Southern Oregon Üniversitesi, dolandırıcıların eğitim kurumunu kontrolleri altındaki bir banka hesabına para aktarması için kandırmasının ardından BEC saldırısının kurbanı olduğunu duyurur. Basında çıkan haberlere göre, üniversite Nisan ayı sonlarında bir banka hesabına 1,9 milyon dolar havale eder. Üniversite bu ödemeyi bir öğrenci eğlence merkezi inşa etmekten sorumlu bir yüklenici olan Andersen İnşaat'a yaptıklarını düşünür ancak söz konusu şirketin ilgili ödemeyi almadığını beyan etmesi üzerine olayın bir dolandırıcılık olduğu ortaya çıkar. Yapılan incelemeden dolandırıcının üniversitedeki projelere hangi inşaat firmalarının dâhil olduğunu tespit ettiği ve ardından üniversiteleri yanlış banka hesabına para aktarmaları için kandırmak için sosyal mühendislik ve e-posta sahtekârlığının bir karışımını kullandığı belirlenir. Yerleşik bir satıcı gibi davranan dolandırıcı, üniversitenin muhasebe ofisine gelecekteki ödemelerde kullanılmak üzere banka hesabı değişiklikleriyle birlikte bir e-posta gönderir, ilgili e-posta üniversitenin mevcut bir iş ilişkisine sahip olduğu bir inşaat şirketinden gelmiş gibi gösterilir.

4.5. Vaka 5 [6]

Porto Riko, 2020 Ocak ayında devlet kurumlarına yönelik üç ayrı BEC saldırısında 4 milyon dolardan fazla kaybeder. Dolandırıcı, Porto Riko'nun İstihdam Emeklilik Sistemindeki bir finans çalışanının e-postası üzerinden harekete geçer. Dolandırıcı, çalışanın hesabını kullanarak,

[4] Bu vaka Demirören Haber Ajansının 03.09.2019 tarihli haberinden alınmıştır.
[5] Bu örnek Cluley (2017) tarafından kaleme alınan "How a Single Email Stole $1.9 Million from Southern Oregon University" adlı haberinden derlenmiştir (Cluley, 2017).
[6] Bu vaka Proofpoint'in 2021 yılında yayınlamış olduğu "You've Got BEC! A Roundup of the 10 Biggest, Boldest, and Most Brazen Business Email Compromise Scams of 2020 and 2019" başlıklı çalışmasından derlenmiştir. Söz konusu çalışmada Associated Press Haber Ajansında çalışan Danica Coto'nun Şubat 2020 tarihinde yayınlamış olduğu "3 employees suspended in $4M Puerto Rico online scam.", "Official: Puerto Rico govt loses $2.6M in phishing scam." başlıklı haberlerinden yararlanılmıştır.

çalışanın diğer kurumlardaki meslektaşlarına e-postalar gönderir. E-postada, alıcılara havale ödemelerine bağlı banka hesap numarasını değiştirme talimatını içerir. Bu BEC tarzı saldırıdır. Dolandırıcı finans çalışanının adresini kullandığı için yalnızca e-posta adresini meşru göstermeye çalışmaz aynı zamanda meşru bir hesap kullanır. En büyük hırsızlık ise adada ekonomik kalkınmaya yatırım yapan devlete ait bir şirket olan Porto Riko Sanayi Geliştirme Şirketi'nin hedef alınması şeklinde ortaya çıkar ve hükümet fonlarında 2,6 milyon dolarlık kayıpla sonuçlanır. Porto Rikolu Turizm Şirketi de 1,5 milyon dolar kaybeder. Bölgenin Ticaret ve İhracat Şirketi ise 63.000 dolar kaybeder. Çoğu BEC saldırısı gibi, Porto Riko'nun savunmasızlığın ana unsuru insandır. Porto Riko'da kâr amacı gütmeyen bir siber güvenlik kuruluşu olan Obsidis Consortia'nın başkanı José Quiñones, Associated Press'e *"Hükümetin büyük ölçüde başarısız olduğu yer teknoloji değil prosedürlerdi"* ifadesini kullanır.

5. BULGULAR

BEC dolandırıcılığında dolandırıcılar, alıcının güvenmesi gereken biri (tipik olarak bir iş arkadaşı, patron veya satıcı) gibi davranır. Gönderici, alıcıdan banka havalesi yapmasını, maaş bordrosunu yönlendirmesini, gelecekteki ödemeler için banka bilgilerini değiştirmesini vb. ister. Standart siber savunmalarla analiz edilebilecek kötü amaçlı yazılım veya kötü amaçlı URL'ler kullanmadıkları için BEC saldırılarını tespit etmek zordur. Bunun yerine, BEC saldırıları, saldırganın adına etkileşimde bulunan insanları kandırmak için kimliğe bürünme ve diğer sosyal mühendislik tekniklerine dayanır. Hedeflenen yapıları ve sosyal mühendislik kullanımları nedeniyle, bu saldırıları manuel olarak araştırmak ve düzeltmek zor ve zaman alıcıdır. BEC saldırıları, etki alanı sahtekârlığı ve benzer etki alanları gibi çeşitli kimliğe bürünme teknikleri kullanır. Bu saldırılar etkilidir çünkü etki alanı kötüye kullanımı karmaşık bir sorundur. Etki alanı sahteciliğini durdurmak yeterince zordur buna ek olarak benzer her potansiyel etki alanını tahmin etmek daha da zordur. Ve bu zorluk, yalnızca, kullanıcıların güvenini sömürmek için bir BEC saldırısında kullanılabilecek bir dış iş ortağının her etki alanıyla artar. BEC ve EAC, teknik güvenlik açıklarından ziyade insan zayıflığına odaklandığından, çok çeşitli BEC ve EAC tekniklerini önleyebilen, tespit edebilen ve bunlara yanıt verebilen insan merkezli bir savunma sistemi gerektirir (Proofpoint, 2020).

Örnek vakalarda da görüldüğü üzere failler herhangi bir olağanüstü çabaya gerek duymadan bazen bir yapay zekâ tabanlı bir yazılım da kullanma yoluyla işletme yöneticisi veya çalışanı gibi davranarak hileli bir işlemi kolaylıkla gerçekleştirebilmektedir. Siber suçlular, finans, muhasebe veya insan kaynakları alanlarında çalışan yöneticileri ve çalışanları hedeflemek için sosyal medyadan, şirket web sitelerinden, dizinlerden, veri tabanlarından vb. halka açık bilgileri kullanır (Bakarich ve Baranek, 2020: 3) ve hedefleri çok geniş bir yelpazeyi kaplar. Diğer bir ifade ile BEC dolandırıcılıkları kamu kuruluşlarından eğitim kuruluşlarına küçük işletmelerden büyük işletmelere kadar çok geniş bir faaliyet alanında gerçekleşmektedir. Dolandırıcıların temel amacı finansal bir kazanç sağlamaktır ve hedef işletmeler ve/veya diğer kuruluşlar olduğundan dolandırıcılar tarafından elde edilen kazanç bireysel dolandırıcılıklar sonucunda elde edilen kazanca göre oldukça yüksek tutardadır. Diğer taraftan BEC dolandırıcılığı sadece kurban işletmeleri veya kuruluşları değil aynı zamanda tedarikçi, satıcı vb. gibi ilişkili tarafları da etkilemektedir. Bu nedenle her bir tarafın korunabilmesi için tüm tarafların e-posta sistemlerinde uygun siber güvenlik kontrollerine sahip olması gerekir. Sadece bir tarafın uygun kontrollere sahip olması yeterli değildir. Bu nedenle, her bir taraf diğer tarafları işlem konusunda eğitmeli ve diğer tarafların da uygun kontrollere sahip olmasını sağlamalıdır (Archie, Turner ve Wybitul, 2020: 14).

6. SONUÇ VE ÖNERİLER

Teknolojik ve dijital gelişmeler dolandırıcıların yöntemlerini farklılaştırmalarına ve geliştirmelerine katkı sağlamıştır. Bu yöntemlerden biri de BEC saldırıları veya dolandırıcılığıdır. BEC saldırıları, birey ya da organizasyonun fark etmeksizin, kurbanların ciddi ekonomik kayıplar yaşamalarına neden olan bir siber saldırı yöntemi olarak dikkat çekmekte ve milyarlarca dolarlık kayıplar yaşanmasına neden olmaktadır. Her ne kadar dolandırıcılık yöntemleri birbirinden farklı olsa da, amaç her zaman ekonomik bir kazanç elde etme, araç ise aldatma eylemini içermesidir. Buna ek olarak aldatma eyleminin başarılı olabilmesi için de daima güvenin tesis edilmesi gereklidir. BEC dolandırıcılığında da kullanılan yöntem bu güveni tesis ederek, kurbanların aldatılması sonunda da ekonomik bir getiri sağlaması şeklinde gerçekleşmektedir.

Klasik bir BEC dolandırıcılığı, görsel açıdan tanıdık görülen bir e-posta adresinden geldiği konusunda çalışanların inandırılmasını amaçlamaktadır. E-postanın ilgili yöneticilerden geldiği konusunda çalışan üzerinde güven oluşturulmasının hemen akabinde dolandırıcılar, çalışanlardan sahte banka havaleleri gerçekleştirmelerini isteyebilir veya kritik bilgilere yanıt vermeleri talep edilebilir. Bu açıdan ele alındığında dolandırıcılar BEC saldırılarında güven tesis ederek oldukça etkili bir yöntemle amaçlarına ulaşabilmektedir.

Hileli eylemler her geçen gün artmakta ve günümüzdeki gelişmelere paralel olarak hile eylemlerinin yöntemi de değişmektedir. Dolandırıcılar stratejilerini ve teknoloji kullanımlarını sürekli yenileyerek gerek işletmeleri gerekse insanları önemli zararlarla karşı karşıya bırakmaktadır. Geçmiş yıllarda klasik bir dolandırıcılık, kurbanın para veya kişisel bilgilerinin ele geçirilmesi için ikna yöntemleri şeklinde gerçekleşirken ki bu durum devam etmekte olsa da günümüzde kurbanlarla çok sınırlı temas kurularak veya hiç temas kurulmadan gerçekleştirilmeye başlandığından dolayı bu tür dolandırıcılıklar konusunda farkındalığın geliştirilmesine ve/veya dolandırılmaktan kaçınılmasını zorlaştırmıştır.

Bu çalışmada BEC dolandırıcılığına ilişkin farklı ülkelerde yaşanmış beş vaka incelenmiştir. Vakalar incelendiğinde ve sonuçlar genel olarak değerlendirildiğinde, işletme yöneticisi veya çalışanı gibi davranarak hileli eylemlerin çeşitli yazılımlar kullanarak kolaylıkla gerçekleştirilebileceği görülmektedir. İşletmeler BEC dolandırıcılığına karşı neler yapabilir? Bu soruya çok sayıda cevap verilebilir. Özet olarak değinmek gerekirse öncelikle işletmelerin günümüzün siber tehdit ortamının durumunu anlaması ve bu durumu kabul etmesi gerekir. Bu tehditlere karşı etkili bir şekilde korunmak için şirketlerin bu tarz saldırılara karşı oluşturulmuş savunma sistemlerine sahip olmaları, diğer taraftan bilgi teknolojilerinin güvenliğinin işletmeler tarafından tesis edilmesi ve gerekli eğitimlerin tüm çalışanlara sağlanması büyük önem taşımaktadır. Şirketlerin siber güvenlik bilinci, önleme ve en iyi güvenlik uygulamalarını tüm organizasyon genelinde yaygınlaştırması, büyük meblağlar içeren fon transferi taleplerinin gerçekliğinin doğrulanması gerektiği bilincinin tüm çalışanlara iletilmesi gerekmektedir. Talebin bir yöneticiden gelmesi gibi bir durumda söz konusu talep *"meşrudur inancı"* yerine *"talep şüpheli olabilir"* şeklinde olaya yaklaşılmalıdır. Bu yaklaşım farklı noktalardan sorgulanırsa bu tarz bir dolandırıcılık kurbanı olma ihtimali azalacaktır. Satıcı veya tedarikçi şüpheli bir şekilde farklı bir ödeme konumu sağlarsa, bunu bir kırmızı bayrak olarak kabul edilmesi gerekmektedir. Örneğin bir tedarikçinin birkaç yıldır çalıştığı bir bankanın aniden değiştirildiğini işletmeye ifade etmesi ve bir para transferinin yeni bankaya veya hesaba yönlendirilmesi talebi, e-posta adreslerinin değiştirildiğinin bilgilendirilmesi önemli bir uyarı sistemi olarak değerlendirilmelidir. Son olarak özellikle e-posta yoluyla yapılan herhangi bir ödeme talebinde çalışanların telefon görüşmesi veya yüz yüze görüşme yaparak gerek sorgulama gerekse doğrulama adımlarını izlemeleri işletme yönetimleri tarafından net bir şekilde politika ve prosedürlerle sağlanmalıdır.

KAYNAKÇA

Archie, J.C., Turner, S. ve Wybitul, T. (2020). *The Pervasive Threat of Business Email Compromise Fraud – and How to Prevent It*. Intellectual Property & Technology Law Journal, 32 (7), 13-15.

Bakarich, K.M. ve Baranek, D. (2020). *Something Phish-y is Going On Here: A Teaching Case on Business Email Compromise.* Current Issues in Auditing, American Accounting Association, 14 (1), 1-9.

Cluley, G. (2017). *How a Single Email Stole $1.9 Million from Southern Oregon University*. https://www.tripwire.com/state-of-security/security-data-protection/single-email-stole-1-9-million-southern-oregon-university/ (Erişim Tarihi: 03. 04. 2021).

Cross, C. ve Gillett, R. (2020). *Exploiting Trust for Financial Gain: an Overview of Business email Compromise (BEC) Fraud.* Journal of Financial Crime, 27 (3), 871-884.

DHA. (2019). *CEO'nun Sesini Taklit Edip 1.4 Milyon Lira Dolandırdılar* https://www.hurriyet.com.tr/ekonomi/ceonun-sesini-taklit-edip-1-4-milyon-lira dolandirdilar-41320401 (Erişim Tarihi: 16. 04. 2021).

European Banking Federation. *Cyberscams: Ceo/Busıness Emaıl Compromıse (Bec) Fraud*. https://www.ebf.eu/ebf-media-centre/cyberscams-ceo-business-email-compromise-bec-fraud/ (Erişim Tarihi: 10.04.2021).

Federal Bureau Of Investigation (FBI). (2015). *Business E-Mail Compromise: An Emerging Global Threat*. August 28.

Federal Bureau Of Investigation (FBI). (2017). *Business E-Mail Compromise Cyber-Enabled Financial Fraud on the Rise Globally*. February 27.

Federal Bureau Of Investigation (FBI). (2018). *Business E-mail Compromise The 12 Billion Dollar Scam*. Alert Number I-071218-PSA, Jul 2012, 2018.

Federal Bureau Of Investigation (FBI). (2019). *Business Email Compromise The $26 Billion Scam*. September 10, 2019.

Federal Bureau Of Investigation (FBI). (2020). *FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic,* April 6, 2020.

Federal Bureau Of Investigation (FBI). (2020). *Internet Crime Report 2020*.

Garuba, G. (2021). *Business Email: Uncompromised – Part One*. https://techcommunity.microsoft.com/t5/microsoft-defender-for-office/business-email-uncompromised-part-one/ba-p/2159900 (Erişim Tarihi: 10. 04. 2021).

Gatefy. (2021). *10 Real and Famous Cases of BEC (Business Email Compromise)*, March 19, 2021.

Gibbs, S. (2017). *Facebook and Google were Conned out of $100m in Phishing Scheme*, The Guardian. 28 April 2017, www.theguardian.com/technology/2017/apr/28/facebook-google-conned-100mphishing-scheme (Erişim Tarihi: 15. 04. 2021).

Lazic, M. (2021). *39 Worrying Cyber Crime Statistics* [Updated for 2021], https://legaljobs.io/blog/cyber-crime-statistics/ (Erişim Tarihi: 05. 04. 2021).

Proofpoint. (2021). *Business Email Compromise (BEC).* https://www.proofpoint.com/us/threat-reference/business-email-compromise (Erişim Tarihi: 08. 04. 2021).

Proofpoint. (2021). *You've Got BEC! A Roundup of the 10 Biggest, Boldest, and Most Brazen Business Email Compromise Scams of 2020 and 2019*.

Sobers, R. (2021). *134 Cybersecurity Statistics and Trends for 2021.* https://www.varonis.com/blog/cybersecurity-statistics/ (Erişim Tarihi: 28. 04. 2021).

Terkoğlu, B. (2020). *Bankadan Milyon Dolar Nasıl Çekilir?.* Cumhuriyet Gazetesi, 30 0cak 2020. (Erişim Tarihi: 04. 04. 2021).

Trend Micro. (2017). *Tracking Trends in Business Email Compromise (BEC) Schemes* (Written by Remorin, L., Flores, R. ve Matsukawa, B.).

Trend Micro. (2018). *Delving into the World of Business Email Compromise (BEC).* https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/delving-into-the-world-of-business-email-compromise-bec (Erişim Tarihi: 01. 04. 2021).

Zweihgaft, D. (2018). *Business Email Compromise and Executive Impersonation: Are Financial İnstitutions Exposed?.* Journal of Investment Compliance, 18 (1), 1-7.