Finans Hukuku Gündemi Dergisi
Sayı 3, Şubat 2020

KRİPTO PARALARA İLİŞKİN DOLANDIRICILIK YÖNTEMLERİ

Av. Ayça AKTOLGA ÖZTÜRK

Günümüzde internetin ve internet üzerinden yapılan işlemlerin yaygınlaşması ile birlikte, dolandırıcılık yöntemlerinin de giderek geleneksel yöntemlerden farklılaştığı ve kapıdan satışlar yoluyla yapılan dolandırıcılık yöntemlerinin yerini internet dolandırıcılığının aldığı görülmektedir.

Bunun en sık rastlanılan örneklerinden biri internet bankacılığı dolandırıcılığı olup, banka müşterilerinin hassas bilgilerinin siber suçlular tarafından telefon, e-mail gibi yöntemlerle ele geçirilmesi suretiyle banka mudilerinin internet bankacılığı hesaplarına izinsiz veya yetkisiz şekilde girilerek hesaplardaki paraların dolaylı yoldan siber suçlulara ait hesaplara aktarıldığı veya kredi kartı bilgilerinin ele geçirilerek siber suçlular tarafından kredi kartının kullanıldığı görülmektedir.

2008 yılından itibaren Bitcoin önderliğinde kripto paraların ve buna bağlı olarak ICO ("Initial Coin Offerings") olarak adlandırılan kripto para arzlarının gündeme gelerek popülaritesinin artması ile birlikte her yeni gelişen teknolojide olduğu gibi bu alan da dolandırıcıların ilgisini çekmiş ve siber suçlular çeşitli dolandırıcılık yöntemleri ile suça konu eylemlerini gerçekleştirmek suretiyle mağduriyet yaratmaya devam etmişlerdir.

Bilindiği üzere, ülkemizde kripto paralara ve blokzincir teknolojisine ilişkin yürürlükte bulunan herhangi bir kanun, yasal düzenleme ve/veya resmi/idari makam kararı bulunmamakta olup, aynı zamanda ülkemizde sayısı 40'ı aşkın kripto para alım satım platformlarına da herhangi bir resmi veya idari bir kuruluş tarafından izin veya lisans verilmemektedir. Bu nedenle, kripto paralar, ICO olarak tabir edilen kripto para arzları ve kripto para alım satım platformları mevzuatın ve idari otoritelerin şimdilik düzenleme alanı dışında kalmaktadır. Bununla birlikte, her ne kadar kripto paralar veya sayılan kurumlar düzenleme kapsamında alınmasa da 5237 sayılı Türk Ceza Kanunu ("TCK") kapsamında hırsızlık ve dolandırıcılık eylemleri suç olarak düzenlenmiştir. Dolayısıyla kripto paralar, ICO'lar veya kripto para alım satım platformları araç olarak kullanılmak suretiyle gerçekleştirilen hırsızlık ve dolandırıcılık eylemlerinin failleri suça ilişkin maddi ve manevi unsurların bulunması halinde TCK kapsamında cezalandırılabilecektir.

Kripto para hırsızlığı veya dolandırıcılığında en sık kullanılan yöntemlere baktığımızda ise internet bankacılığı ve kredi kartı dolandırıcılığına benzer bir yapı olduğu gözlenmekle birlikte kripto paraların doğası gereği farklı dolandırıcılık tipleri de karşımıza çıkmaktadır. Bu dolandırıcılık yöntemleri arasında önemli görülenler aşağıdaki gibi sıralanmıştır:

Sosyal mühendislik

Sosyal mühendislik, temeli insana dayanan dolandırıcılık yöntemlerinden birisi olup bu dolandırıcılık yönteminde siber suçlular hedefledikleri kişiden istedikleri bilgileri almak

veya hedefledikleri kişinin kripto paralarını çalmak amacıyla taklit, etkileme ve ikna etme kabiliyetlerini kullanmaktadırlar.

Bahse konu yöntemler arasında, internet sitelerinde normalden daha uygun fiyatlı teknolojik alet satılması, yüksek miktardaki Bitcoin, etherium cinsinden kripto paraların aktarılmasına yardımcı olunması karşılığında kişiye ödül vaat edilmesi, ölmüş bir kişinin sahip çıkılmamış parasının gönderilmesi için masrafların yabancı ülkeye daha kolay ve masrafsız olması gerekçesiyle kripto para yoluyla gönderilmesinin talep edilmesi, ödül, piyango içerikli e-posta mesajları gibi örnekler bulunmaktadır.

Kişiye normalde 10.000,-TL fiyatlı bir telefonun 3.000 - 4.000,-TL karşılığa denk gelecek kripto para ile satılmak istenmesi örneğinde, kişi satın almak istediği telefon için kendisine verilen sanal cüzdan adresine ilgili kripto paraları gönderir ancak karşılığında aldığı telefon yerine eski bir cihaz gönderilmekte veya herhangi bir telefon gönderilmemektedir.

Zararlı Yazılım

Masaüstü bilgisayar, cep telefonu ve tablet gibi cihazları hedef alan ve içerisinde zararlı unsurlar barındıran yazılımlardır.

Siber suçlular tarafından kripto para alım satım platformlarının, sanal cüzdan hizmeti sağlayan platformların uygulamaları taklit edilmekte, müşterilerin/kullanıcıların bu uygulamalara kimlik, parola ve şifre gibi bilgilerini girmesiyle birlikte siber suçlular tarafından müşterilerin/kullanıcıların asıl kripto para alım satım platformları veya sanal cüzdan hizmeti sağlayan platformlara ilişkin bilgileri ele geçirilmektedir. Ele geçirilen bu bilgiler yoluyla ise müşterilerin/kullanıcıların hesaplarına izinsiz olarak girilip, hesaplarda bulunan varlıklar doğrudan ve/veya dolaylı yoldan siber suçlulara ait hesaplara aktarılmaktadır.

Bununla birlikte, kullanıcılara gönderilen e-posta, SMS içeriğinde veya ekinde bulunan zararlı yazılımlar kişilerin gönderilen mesajdaki linki veya eki açmaları suretiyle bilgisayarlarına, telefonlarına veya tabletlerine yüklenebilmektedir. Bahse konu zararlı yazılımlar çoğu zaman geri planda müşterinin/kullanıcının kripto para adresini herhangi bir yere girmesini/kaydetmesini beklemekte olup, bu yazılımlar ile müşterinin/kullanıcının kripto paralarını transfer etmek istediği sanal cüzdan adresleri yerine siber suçluların kendi sanal cüzdan adreslerinin yazılması sağlanmaktadır. Bahse konu sanal cüzdan adresleri 27 ile 34 arasında sayı ve harften oluşan örneğin; 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa gibi komplike adresler olduğundan transfer işlemini gerçekleştiren kişinin dikkatinden kolayca kaçabilmekte ve asıl gönderilmek istenilen sanal cüzdan adresleri yerine zararlı yazılım tarafından kopyalanan/yüklenen adrese kripto para transferleri sağlanmaktadır.

Phishing (Oltalama) Saldırıları

Bu saldırı tipinde siber suçlular, kripto para alım satım platformlarının, sanal cüzdan hizmeti sağlayan platformların veya ICO'ların asıl internet sitesiymiş gibi hazırladıkları sahte

internet siteleri veya bahse konu kurumları taklit ederek hazırlanan sahte e-postaları, elde edebildikleri tüm e-posta adreslerine göndermektedirler.

Bahse konu sahte internet siteleri çoğu zaman asıl site ile benzerlik arz ettiğinden (www.google.com olan bir alan adının www.gooogle.com olarak kullanımı) ve/veya arama motorlarında satın aldıkları öne çıkmaya ilişkin reklamlar yoluyla arama motorlarında üst sıralarda yer aldıklarından internet sitesinin adres çubuğunda yazan bilgilere dikkat etmeyen müşteriler/kullanıcılar tarafından karıştırılmaktadır. Müşterilerin/kullanıcıların sahte internet sitelerine hesaplarına girmek üzere kimlik, parola ve şifre gibi bilgilerini vermesiyle birlikte siber suçlular tarafından müşterilerin/kullanıcıların bilgileri ele geçirilmekte, eş zamanlı olarak siber suçlular elde ettikleri bu bilgiler ile arka planda asıl internet sitelerinde müşterilerin/kullanıcıların hesaplarına girerek hesaplarda bulunan varlıkları doğrudan ve/veya dolaylı yoldan siber suçlulara ait hesaplara aktarmaktadır.

Sahte e-postalarda ise; bu e-postaların konusu, müşterilerin/kullanıcıların bilgilerinin güncellenmesi veya şifrelerin değiştirilmesi amacı içeren ifadelerden ve/veya sayılan kurumların birebir kopyası şeklinde görünen internet sayfalarına giden linklerden oluşmaktadır. E-postanın gönderildiği e-posta adresine dikkat etmeyen müşteriler/kullanıcılar ise mesajda talep edilen bilgileri doldurarak e-postalara cevap vermek veya gönderilen linke tıklamak suretiyle bu linkte talep edilen bilgileri doldurarak kişisel bilgilerinin ve şifrelerinin siber suçlulular tarafından ele geçirilmesine yol açarlar.

Bilgisayardaki Verilerin Hacklenmesi ile Veriler Karşılığında Kripto Para Talep Edilmesi

Bahse konu dolandırıcılık yönteminde siber suçlular tarafından sosyal mühendislik yöntemleri uygulanmak suretiyle e-posta mesaj içeriğinde gönderilen linkin veya ekinde gönderilen belgenin kişi tarafından açılması veya internet sitesinden zararlı yazılım yüklemesi gibi yöntemlerle özellikle şirketlerin bilgisayar sistemlerine sızılmaktadır. Bilgisayar sistemine sızan siber suçlular şirketlerin veya kişilerin bilgisayarlarında yüklü tüm verileri şifrelemekte ve ilgili verileri ulaşılamaz hale getirmektedir. Kişinin verilerine ulaşmak istemesi halinde ise, siber suçlular tarafından belirtilen sanal cüzdan adreslerine kripto para göndermesi talep edilmektedir. Belirtilen sanal cüzdan adreslerine kripto para gönderilmesi halinde siber suçlular verilere erişim için gerekli şifreleri ilgili kişi ile paylaşabildikleri gibi bu bilgileri hiçbir zaman paylaşmayabilmektedirler.

ICO'lar Yoluyla Yapılan Dolandırıcılık Eylemleri

ICO (ilk kripto para arzı), geleneksel yatırımlardaki IPO'ya (ilk halka arz) veya son dönemde ülkemizde de düzenleme alanı bulan kitle fonlamasına (crowdfunding) çok benzeyen, bir şirketin sunacağı yeni bir hizmet veya ürün karşılığında halktan para/fon toplaması yöntemini kullanan ve kendi yatırımını toplanan bu para/fonlarla finanse etmenin amaçladığı bir yöntemdir. Yatırımcı olarak tabir edilen kişilerden toplanan para/fon karşılığında ilgili yatırımcı belirli sayıda kripto parayı edinmektedir. Bu halihazırda kullanılan

kripto paralardan olabileceği gibi fonu toplayan şirket tarafından ihraç edilen yeni bir kripto para da olabilir.

Yatırımcılar; bu kripto paraları yaptıkları yatırımların değerleneceği gayesiyle edinmektelerse de piyasadaki kötü niyetli ICO'lar sebebiyle mevcut yatırımından zarar eden veya mevcut yatırımını tümüyle kaybeden çok sayıda yatırımcı bulunmaktadır. Kripto paralar ve kripto para arzları halihazırda regülasyona tabi olmadığından hukuki anlamda yatırımcıların korunması da pek mümkün olmamaktadır. Bloomberg için SATIS Group tarafından yapılan bir araştırmaya göre, ICO'ların %78'lik kısmı sahtekarlık maksatlı, %4'ü başarısız, %3'ü ölmüş, ancak %15'i değişim bazlı bir ticarete konu olabilmiştir. Bu istatistik bir yatırımcı için pek iç açıcı ve güvenilir değildir.

Bu durumun yakın zamandaki örnekleri arasında OneCoin isimli ICO ve ihraç ettiği aynı adlı kripto parası örnek olarak verilebilir. Zamanla OneCoin'in sanal para sisteminden ziyade aslında bir 'saadet zinciri' olduğu anlaşılmış olup, ortalama 3 milyon kişinin üye olduğu OneCoin sistemiyle yatırımcılardan yaklaşık 3.8 milyar dolar değerinde para toplanmıştır. Şirkete ve şirketin yöneticilerine yönelik uluslararası soruşturmalar ve davalar halen devam etmekte olup, çeşitli ülkelerde açığa çıkan skandallar OneCoin'in büyük bir soygun olduğunu ortaya koymaktadır.

Bu nedenle, yatırımcıların ICO'lara yatırım yaparken çok iyi değerlendirme yapmaları gerekmekte olup, gerekli araştırmayı yapmadıkları takdirde yatırmış oldukları anaparalarını tümüyle kaybetme riskini göze almaları gerekmektedir.

Bununla birlikte, bahse konu ICO'lar tarafından ihraç edilen ve aslında değeri olmayan kripto paraların listelenerek bazı kripto para alım satım platformlarında satıldıkları da görülmektedir. Bahse konu kripto parayı alan kişi eğer gerekli araştırmayı yapmamışsa ikinci elde aldığı kripto para için ödediği parasının bir kısmını veya tümünü kaybetme riskiyle karşı karşıya kalabilir.

Bahse konu ICO'ların dolandırıcılık veya suça konu eylemlerinin söz konusu olmaları halinde ise yatırımcıların paralarını kaybetmeleri dışında suça karışma tehlikeleri de bulunmaktadır. ICO'ların çoğunun merkezinin nerede olduğu bilinmediği gibi, bu ICO'lara hangi ülkenin hukukunun da uygulanacağı çoğu zaman belirsizdir. Bu nedenle halka arz niteliği taşıyan ICO'ya yatırdığı para ile ICO'nun ortağı olan ve karşılığında kendisine belirli oranda kripto para vaat edilen bir yatırımcı, bahse konu ICO'nun bahis oynanması, uyuşturucu ticareti yapılması vb. gibi yasa dışı işlerle iştigal etmesi halinde kendisini hiç bilmediği bir ülkenin hukukuna göre bir ceza dosyasının şüphelileri arasında bulabilecektir.

Dolandırıcılık Amacıyla Kurulan Kripto Para Alım Satım Platformları

Kripto para alım satım platformları yasal otoriteler tarafından düzenlenmediğinden sadece teknik hususlar konusunda bilgisi olan kişiler tarafından kurulmaları ve faaliyete başlamaları bir hayli kolaydır. Herhangi bir oranda sermaye yeterliliği, anonim şirket şeklinde kurulmuş olma zorunluluğu veya kurucuların belirli şartları taşımaları gibi zorunluluklar bulunmamaktadır. Bu nedenle, kötü niyetli kişilerce kurulan kripto para alım satım

platformları yoluyla bu platformlara müşteri olan kişilerin kripto paralarının veya fonlarının çalınması riski bulunmaktadır.

Bunun tarihteki en ünlü örneklerinden birisi Mt. Gox vakası olup, Tokyo merkezli kripto para borsası olan ve 2010 yılında kurulan Mt. Gox, 2014 yılında dünya çapındaki tüm Bitcoin işlemlerinin yüzde 70'ini gerçekleştirmekteydi. Ancak 2014 yılında yaşanan siber saldırı neticesinde müşterilerinin 473 milyon dolar değerindeki kripto paralarını kaybetmişti. Bahse konu olayla ilgili olarak anılan kripto para borsasının CEO'su Mark Karpeles hakkında, Mt. Gox'un yaklaşık 3 milyon dolar değerindeki parasını zimmetine geçirdiği ve borsanın kasa bakiyesini şişirmek için kayıtları manipüle ettiği iddiaları ile soruşturma başlatılmıştır. Nitekim, kapanan ve müşterilerinin kripto paralarını çalan kripto para borsalarına ilişkin haberlere halen rastlanılmaktadır.

Bu nedenle, kişilerin kripto para alım satımını yapacakları kripto para alım satım platformlarını iyice araştırmaları önem kazanmaktadır. Müşterilerin, işlem yapacakları kripto para alım satım platformlarında sermaye yapısı, yönetim ve üst düzey yöneticiler, müşteriyi tanıma (KYC) kuralları, komisyonlar, kurulu bulunduğu/yerleşik olduğu ülke gibi hususlara dikkat etmeleri önemlidir. Özellikle ülkemiz dışında kurulu kripto para alım satım platformlarına para yatıran müşterilerin; bahse konu bu platformların müşterilerini dolandırarak kapandığı veya müşterilerine paralarını ödemekten imtina ettikleri zaman alacaklarına kavuşmak için platformun kurulu bulunduğu ülkede adli süreçlere girişerek yabancı bir ülke hukukuna göre yapılacak yargılamaların sonucunu beklemeleri gerekmektedir. Uzun ve masraflı olan bu sürece girmek istemeyen müşterilerin ise mağduriyet yaşamaları kaçınılmazdır.

Ülkemizde 6102 sayılı Türk Ticaret Kanunu'nun ilgili maddeleri uyarınca, sermaye şirketi şeklinde kurulan anonim şirket ve limited şirketlerde şirket ortaklarının şirket borçlarından sorumluluğu münhasıran taahhüt ettikleri sermaye ile sınırlıdır. Bu nedenle, müşterilerin kripto para alım satımını yaptıkları platformların şirket sermayelerini kontrol etmelerinin de yararlı olacağı düşünülmektedir. Bahse konu bilgiler kamuya açık Türkiye Ticaret Sicil Gazetesi yoluyla edinilebileceğinden kısa bir zamanda yapılacak araştırma uzun vadede müşterinin kendisini korumasını sağlayacaktır.

Yukarıda bahsedilen tüm dolandırıcılık yöntemlerinde en dikkat çekici unsur genelde siber suçlular tarafından kullanılan sanal cüzdan hesaplarındaki hareketliliktir. Mikser, bir diğer deyişle karıştırma olarak tabir edilen bu işlemlerin amacı sanal cüzdanlar ve sahipler arasındaki bağlantıların izlenmesinin engellenmesini sağlamak ve kripto paraları alan ve gönderen adresler arasındaki bağlantının kurulmasını engellemektir. İşlemler, havuz hesap olarak tabir edilen sanal cüzdan hesaplarında karıştırıldıktan sonra küçük miktarlar şeklinde bu hesaplardan başka onlarca veya yüzlerce sanal cüzdan hesaplarına transfer yapılmakta, böylece işlemlerin izlenmesinin imkansız hale getirilmesi hedeflenmektedir. Kripto paraların transfer işlemlerinin blokzincir üzerinde kamuya açık olarak kaydedilmesi sonucu mikser (karıştırma) özelliği siber suçluların dolandırıcılığa konu kripto paraların izinin sürülmesini engellemek amacıyla başvurdukları yollardan birisi olmuştur. Teknolojinin ilerlemesiyle

birlikte geliştirilen programlar sayesinde günümüzdeki siber suçlulukların kullandığı bu karıştırma yönteminin takibi yapılabilmektedir.

Yazıda kripto paralara ilişkin önemli olduğu ve sıklıkla karşılaşıldığı düşünülen dolandırıcılık yöntemleri konusunda özet niteliğinde bilgi verilmeye çalışılmıştır. Kripto paralara ilişkin dolandırıcılık yöntemleri sayılanlarla sınırlı olmadığı gibi önümüzdeki günlerde sektörün giderek çeşitlenmesi ve blockchain (blokzincir) uygulamalarının da artmasıyla birlikte dolandırıcılık yöntemlerinin de giderek farklılaşacağı öngörülmektedir.