Ortadaki Adam Saldırısı (Man in the Middle Atack) Yolu ile Dolandırıcılık

30.04.2021

1. Son yıllarda ülkemizde de sık sık görülen nitelikli dolandırıcılık yöntemlerinden biri "Ortadaki Adam Saldırısı (Man in the Middle Atack)" olarak adlandırılmaktadır. E-posta yazışmaları üzerinden yapılan bu dolandırıcılık yöntemi en yalın anlatımı ile şu şekilde özetlenebilir:

a. Geniş bir ağa sahip internet korsanları (hacker) uluslararası ticaret yapan şirketleri önce dışarıdan izleyerek şirket yetkililerinin davranışlarını ve hareketlerini gözlemlemeye başlıyorlar.

b. İki şirket arasındaki e-posta yazışmalarını takip edip, şirket yetkililerinin birbirlerine hitap şekillerini, şirketlerin ödeme tarihlerini vb. konuları takip ediyorlar.

c. Örnek olsun; A şirketi ile B şirketi arasında aylık bir ticari ilişki olduğunu kabul edelim. A şirketi her ay B şirketine 100.000 USD'lik bir mal sattığını varsayalım. İnternet korsanları aylarca süren izleme takipleri ile bunu önce keşfediyorlar. **Sonra da şirket yetkililerinin davranışlarını öğrenip, A şirketinin yetkilisinin e-posta adresini tamamen kırarak ve onun yerine geçerek B şirketinin yetkilisine e-posta gönderiyorlar.**

d. Bu e-postada A şirketinin yetkilisiymiş gibi ve onun ağzından 100.000 USD'lik faturayı gönderiyorlar ancak bu sefer, **ödeme yapılacak banka hesabının farklı bir IBAN'a yatırılması talebini sunuyorlar.** B şirketi yetkilisi de uzun zamandır ticaret yaptığı A şirketi yetkilisinin bu talebinden şüphelenmeyerek, **internet korsanlarının istediği hesaba 100.000 USD'yi gönderiyor.**

e. Devamında şayet bu yatan para bankadan nakit olarak çekilebilecekse, internet korsanları çok hızlı bir şekilde bankadan bu parayı nakit olarak çekerek, ortadan kayboluyorlar.

2. Bir yöntemi yukarıda anlattığımız şekilde olmakla birlikte, buna benzer başka yöntemlerle de "Ortadaki Adam Saldırısı" düzenleyerek, çok yüksek meblağlarda dolandırıcılık yoluna girişilmektedir. Yöntem dışında uygulamada karşılaştığımız ihlaller ya da şirket yetkililerinin atladığı hususları da aşağıda sıralamamız gerekir.

a. Uluslararası şirketlerin Dünyanın birçok yerinde şubelerinin ve banka hesaplarının olması beklenebilmektedir. İnternet korsanları bu durumu bildiklerinden, bunu lehlerine çevirerek,

dolandırılan şirket yetkililerinin şüphe duymamalarını sağlamaktadırlar. Örnek olsun; ABC LLC. isimli bir firmanın Hollanda'da faaliyet gösterdiği ve bu firmanın İsviçre'de banka hesabı bulunduğunu varsayalım. İnternet korsanları dolandırıcılığı gerçekleştirmek için, öncelikle ABC LLC. ismi ile örneğin Güney Kore'de bir firma kurarak, orada da banka hesabı açarak, e-posta hesaplarını ele geçirdikten sonra parayı gönderecek firmaya IBAN gönderirken, **kendilerinin Güney Kore'de kurdukları aynı isimli ABC LLC. isimli firmanın Güney Kore'deki hesabına paranın gönderilmesini talep edebiliyorlar. Dolandırılan firma da, ticaret yaptığı ABC LLC. firmasının Güney Kore'de de bir firma ya da şube kurduğunu düşünerek ve firma unvanı aynı olmasından dolayı bu durumdan şüphelenmeyerek parayı Güney Kore'de bulunan hesaba gönderebiliyor.**

b. İnternet korsanları bazı durumlarda ticaret yapan iki firmanın e-posta adreslerini tamamen kıramayabiliyorlar. Ancak yine de yazışmaları izleyerek, uygun zamanda müdahale imkânı kolluyorlar. **Müdahale edip, bir ödemeyi kendilerine yönlendirmek için bu sefer, parayı alacak firma yetkilisinin kullandığı e-posta adresine çok benzer (sadece birkaç harf değişikliği ile) bir e-posta adresi alarak ve e-posta adresi üzerinden yazışma yaparak da şirketleri dolandırabiliyorlar.**

c. Bunun dışında ülkemizde çok rastlanan başka bir durum ise, sahte pasaportlar ile dolandırıcılığa konu paraların çekilmesi şeklinde olabiliyor. Yukarıdaki örnekten hareket edersek, internet korsanları bu sefer sahte bir pasaport hazırlayıp, **pasaport sahibinin *"ismini: ABC; soy ismini de: LLC"* yaparak, bu pasaport ile Türk Bankalarında şahsi döviz mevduat hesabı açıyorlar.** Açılan hesap adı, sahte pasaportta yer alan ad ve soyad olduğundan "ABC LLC" olarak görünmektedir. Sonrasında dolandırılan şirkete internet korsanları Türkiye'de bulunan ve hesap adının "ABC LLC" olduğu IBAN numarası gönderdiklerinde, dolandırılan şirket, şirket unvanı değişmediği için yine bu durumdan şüphelenmeyerek parayı Türkiye'ye yollamaktadır.

d. Ülkemizde maalesef bankacılık uygulamalarının zayıflığı nedeni ile, hem yukarıda bahsettiğimiz sahte pasaport ile hesap açma hadiselerinin *(sahte pasaportta yazan ad-soyad bölümünde görünen isimler çok saçma ya da akıl dışı olsa da -Coca Cola LLC, Michael Jordan gibi- gerçekten geçmişte bu isimlerle hesaplar açıldığı görülmüştür)* hem de çok yüksek meblağlar ile bankadan nakit para çekiminin yapıldığı gözlemlenmiştir. Hatta belirtmek gerekir ki, yabancı olan internet korsanları ile yapılan görüşmelerde, neden ülkemizin bu tür dolandırıcılıkta aracı olarak kullanıldığı sorulduğunda, cevaben; ***"Dünyada bankadan nakit olarak para çekilebilen en kolay ülke Türkiye"*** şeklinde yanıt alındığı da olmuştur.

e. Dolandırılan paranın izini kaybettirmenin bir başka yolu ise, parayı birçok parçaya bölerek ve farklı farklı ülkelere transfer ederek, takibini imkânsız kılmak ile yapılmaktadır. Örnek olarak, İsveçli bir firma dolandırıldığında, ilk olarak paranın Hong Kong'taki paravan bir firmaya gönderilmesi sağlanmakta, ondan sonra bu para dörde bölünerek; Çin, İsviçre, Hollanda ve İngiltere'de bulunan yine paravan firmaların hesaplarına gönderilebilmektedir.

f. Uygulamada yaptığımız araştırmalardan birinde, İsviçre'de bulunan ve dolandırıcılığa karışan paravan bir şirketin banka hesaplarını inceleme fırsatı bulmuştuk. Hesap hareketlerine baktığımızda, Dünyanın tüm bölgelerinden birçok firmanın dolandırıldığı ve paraların Dünyanın birçok ülkesinden bu firmaya geldiği ve genellikle hiç bekletilmeden yine Dünyanın birçok farklı ülkesine gönderildiğini gördük. Hatta yerel makamlarla yaptığımız görüşmelerde, bu tür dolandırıcılığın, uyuşturucu ticaretinin önüne geçtiğini, masrafının çok daha az olduğunu, internet korsanlarının belli mafya gruplarının kontrolünde olduğunu ve **tek bir paravan şirketin dolandırıcılık hacminin yılda 100 milyonlarca Eurolara kadar çıkabildiğinden bahsetmişlerdir.**

3. Tüm bu yöntem ve gelişmelere değindikten sonra, bu nitelikli dolandırıcılık suçuna ilişkin ülkemiz mevzuatına değinmemiz gerekecektir. 5549 sayılı Kara Paranın Önlenmesine Dair Kanun uyarınca, finans kuruluşlarına (yükümlüler) sorumluluklar yüklenmektedir. Kanunda yazımız konusunu ilgilendiren bölüm ikinci bölüm olup, **kanunun 4. maddesi "Şüpheli işlem bildirimi"** başlığını taşımaktadır. 4. maddenin birinci fıkrası şu şekilde düzenlenmiştir;

> ***"Şüpheli işlem bildirimi***
> ***MADDE 4 –*** *(1) Yükümlüler nezdinde veya bunlar aracılığıyla yapılan veya yapılmaya teşebbüs edilen işlemlere konu malvarlığının yasa dışı yollardan elde edildiğine veya yasa dışı amaçlarla kullanıldığına dair herhangi bir bilgi, şüphe veya şüpheyi gerektirecek bir hususun bulunması halinde bu işlemlerin yükümlüler tarafından Başkanlığa bildirilmesi zorunludur."*

Burada finans kurumlarına, kurumları ile ilgili bir para hareketinde, bu paranın yasa dışı yollarla elde edildiğine veya yasa dışı amaçlarla kullanıldığına ilişkin şüphe duyulması halinde, MASAK'a "şüpheli işlem bildirimi"nde bulunma zorunluluğu getirmiştir. Yine aynı kanunun 19/A maddesi uyarınca bu şekildeki bir şüpheli işlem durumunda ilgili **Bakan'ın ya da Bakan'ın vereceği yetki ile Bakan Yardımcısı'nın bu işlemi yedi iş günü boyunca durumu yetkili makamlara bildirmek için askıya alma yetkisi bulunmaktadır.**

Ayrıca *"Suç Gelirlerinin Aklanmasının ve Terörizmin Finansmanının Önlenmesi Kapsamında İşlemlerin Ertelenmesine Dair Yönetmeliğin"* 4/1. maddesine göre ise;

> *"Yükümlüler nezdinde veya bunlar aracılığıyla yapılmaya teşebbüs edilen ya da halihazırda devam eden işleme konu malvarlığının aklama veya terörizmin finansmanı suçu ile ilişkili olduğuna dair şüpheyi destekleyen belge veya ciddi emare bulunması durumunda, yükümlülerin şüpheli işlem bildirimini Başkanlığa gerekçeleri ile birlikte işlemin ertelenmesi talebi ile gönderirler."*

Bir başka ifadeyle ve kısaca, banka yukarıda arz ettiğimiz üzere finans kurumu olan yükümlü, bir e-posta dolandırıcılığı durumunda şüpheli bir para transferi gördüğünde derhal MASAK'a bu durumu bildirmeli ve hızlıca yapılan inceleme sonucunda Bakan ya da yardımcısı yedi iş günü boyunca hesaba bloke koymalı ve ilgili Cumhuriyet Başsavcılığına durumu bildirmelidir. **Bunun dışında Yönetmelik uyarınca suç işlendiğine ilişkin ciddi emare varsa, inisiyatif alarak hesaba bloke koymalı ve durumu MASAK'a bildirmelidir.** İşleyiş bu şekilde gerçekleşirse, ülkemizde yaşanan birçok e-posta yolu ile dolandırıcılığın önüne geçilmiş olur.

4. Kanun dışında Hazine ve Maliye Bakanlığının web sitesinde yayınlanan ve ayrıca MASAK tarafından ilgili yükümlülere gönderilen **"Şüpheli İşlem Bildirimi Rehberi"** bulunmaktadır. Bu rehberde yükümlülere (finans kuruluşları diyebiliriz) hangi işlem ve davranışların şüpheli işlem olabileceğine ilişkin ayrıntılı açıklamalar sunulmaktadır. Örnek olarak rehbere göre, 10.000 TL sermaye ile yeni kurulmuş bir şirketin, bir banka şubesinde mevduat hesabı açıp, ilk işleminin milyon dolarlık bir para transferi olması sonrasında, şirket yetkililerinin bu gelen parayı nakit olarak çekmek istemeleri şüpheli işlem olarak nitelendirilebilecektir.

Ancak ülkemizde finans kurumlarının kendilerine gönderilen bu rehbere riayet ettiklerini söylemek ne yazık ki mümkün değildir. Finans kurumları şüpheli işlemlere dikkat etmediklerinden dolayı, internet korsanları eylemlerini ülkemizde yürütmeye devam etmektedirler.

Av. Kazım Yiğit Akalın