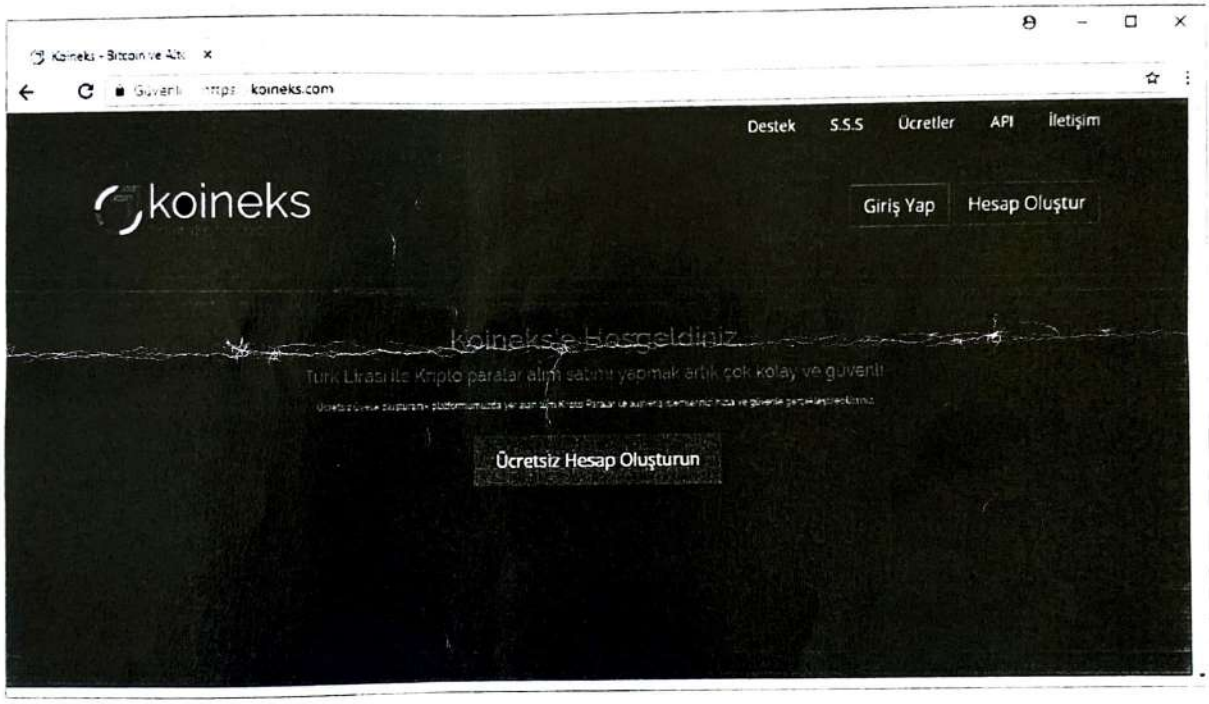
RAPOR

TESPİTİN KONUSU:

İstanbul Cumhuriyet Başsavcılığı tarafından yürütülmekte olan **2018/59986** sayılı soruşturma kapsamında ve yürütülmekte olan hazırlık soruşturmasına esas olmak üzere; **Koineks Teknoloji A.Ş.** İsimli firmaya ait olan ve Kripto Para Al Sat işlemlerinin yapıldığı www.koineks.com isimli web sitesinin bilişim sistemine hukuka aykırı olarak girilmesi, sistemin engellenmesi, sistemin bozulması ve akabinde sistem dâhilinde bulunan kripto paraların nitelikli hırsızlık suretiyle başka cüzdanlara aktarma emri verilerek çalınması olayı ile alakalı olarak, **03.05.2018** günü saat **08.50** ile saat **13.00** arasında, sistemin yönetildiği **Merkez Mah. Akar Cad. ITover Bomonti No:3/60 Şişli** adresinde yerinde inceleme işlemi yapılmıştır. Yapılan incelemeler neticesinde aşağıda detayları bulunan tespitlere ulaşılmış ve suça konu eylemi gerçekleştiren şüpheli şahısların tespit edilebilmesi amacıyla sanal ortamda çalışma başlatılmıştır.



DEĞERLENDİRME ve TESPİTLER:

Soruşturmaya konu olay hakkında, maddi delillere ulaşma amaçlı olarak yapılan yerinde inceleme işlemi sırasında şu tespitlere ulaşılmıştır;

- İlgili bilişim sisteminin internet erişim logları, error logları, PHP MyAdmin logları ve ssh auth logları incelendiğinde, 46.20.11.42 (Mysql), 46.20.11.50 (Web-LiteSpeed), 89.107.227.74 (AdminPanel), 89.107.227.226 (HotWallet), 46.20.14.82 (Kripto Para Hesaplama Motoru), 46.20.14.42 (Kripto Para Hesaplama Motoru Kuyruk Yöneticisi), 46.20.14.66 (Websocket), 46.20.14.34 (Hata Kontrol Alarm, Alış Veriş Geçmişi), 37.247.104.114 (REDIS), 37.247.100.226 (Matc Eng. SQL) sunucularına sürekli siber saldırılar olduğu ancak sistemin güvenlik düzeyi sayesinde adları geçen sunuculara herhangi bir yetkisiz erişim yapılamadığı anlaşılmıştır.

- Suça konu olayda başarılı gerçekleşen siber saldırı eyleminin ise, 12.02.2018 günü saat 08.34 sıralarından itibaren müşteki firmaya ait 138.68.181.237 IP numaralı ve sistemin testi için kullanılan Linux işletim sistemi kurulu sunucu bilgisayara root yetkili SSHD bağlantı denemeleri ile başladığı görülmüştür. 138.68.181.237 Ip Numaralı sunucu bilgisayara yapılan SSHD bağlantı saldırılarının 18 gün sonra 01.03.2018 günü saat 17:30 sıralarında başarılı olduğu ve saldırıyı yapan internet kullanıcısının test sunucusuna root yetkisi ile login olduğu anlaşılmıştır. Akabinde, şüpheli şahsın 05.03.2018 günü saat 06.50 sıralarında asıl sisteme ait 46.20.11.42 (Mysql) IP numaralı sunucu bilgisayara, test sunucusunun bilişim sisteminden elde edilen Mysql kullanıcı adı ve şifresi ile PHP MyAdmin bağlantısı yaptığı ve artık bu sunucuya süreli erişim yaparak, 03.05.2018 günlü tutanak yazım tarihi itibariyle toplamda, 23397531,68 DOGE, 90658 Riple XRP, 104,00712309 BTC, 891,124 ETH, 870,7837418 LTC, 190,4846578 DASH kripto paranın müştekinin bilişim sisteminden çalındığı görülmüş, yine tutanak yazım tarihi itibariyle çalınan kripto paraların TL karşılığının 9.633.471 TL olduğu anlaşılmıştır. Sistem logları incelendiğinde, şüpheli şahsın elde etmiş olduğu veri tabanı erişim yetkisi sayesinde, www.koineks.com isimli web sitesinin üyelerinin şifre bilgilerini değiştirerek ve kendi Google Authenticator kodunu da direk veri tabanına yazarak sisteme başarılı loginler gerçekleştirdiği tespit edilmiş, yapılan bu loginler sonucunda tutanak ekinde detayları bulunan cüzdanlara kripto para çıkışları yaptığı anlaşılmıştır.

- Suça konu eylemi gerçekleştiren şüpheli şahsın www.koineks.com isimli web sitesinin bilişim sistemine yapmış olduğu saldırı sırasında aşağıda detayları bulunan IP numaralarını kullandığı anlaşılmıştır. Bu IP numaraları, Lokasyon ve Servis Sağlayıcısı bilgileri şunlardır;

    - IP: **42.200.253.67** (Hong Kong). 01.03.2018 günü saat 17.30 sıralarında test sunucusuna ilk başarılı root yetkili SSHD bağlantı işlemini gerçekleştiren IP numarası. İlgili Ip numarasının servis sağlayıcının (ISP), "**39/F PCCW Tower, Taikoo Place Quarry Bay Hong Kong**" adresli "**Hong Kong Telecommunications (HKT) Limited**" isimli firma olduğu tespit edilmiştir.

    - IP: **113.68.130.117** (China, Guangdong, Guangzhou). 01.03.2018 günü saat 17:27 sıralarında ve sonraki günlerde test sunucusuna başarılı root yetkili SSHD bağlantı işlemlerini gerçekleştiren IP numarası. İlgili Ip numarasının servis sağlayıcının (ISP), "**No.31 ,Jingrong street, 100032 Beijing China**" adresli "**China Telecom**" isimli firma olduğu tespit edilmiştir.

    - IP: **222.67.214.87** (China, Shanghai, Shanghai). 06.03.2018 günü saat 05.55 sıralarında ve sonrasında test sunucusuna başarılı root yetkili SSHD bağlantı işlemlerini gerçekleştiren IP numarası. İlgili Ip numarasının servis sağlayıcının (ISP), "**No.31 ,Jingrong street, 100032 Beijing China**" adresli "**China Telecom**" isimli firma olduğu tespit edilmiştir.

    - IP: **101.37.163.24** (Zhejiang, China). 07.03.2018 günü saat 21.45 sıralarında ve sonrasında kripto para çekim işlemlerini gerçekleştiren IP numarası. İlgili Ip numarasının servis sağlayıcının (ISP), "**5F, Builing D, the West Lake International Plaza of S&T No.391 Wen'er Road, Hangzhou, Zhejiang, China, 310099**" adresli "**Aliyun Computing Co. LTD**" isimli firma olduğu tespit edilmiştir.

- Yukarıdaki IP numaraları analiz edildiğinde, www.koineks.com isimli web sitesinin bilişim sistemine yapılan siber saldırının, mevcut güvenlik tedbirlerine rağmen, toplamda 18 gün sistem açığı taraması ve test sunucusunun hack edilmesi neticesinde, ÇİN HALK CUMHURİYETİ lokasyonlu internet kullanıcısı ya da kullanıcıları tarafından gerçekleştirildiği açıkça görülmektedir.

- Müşteki işletmede 03.05.2018 tarihinde gerçekleşen yerinde inceleme işlemi sırasında tutulan tutanak ve eklerinde bulunan kripto para transferlerine ait transferlerin hareketleri sanal ortamda incelenmiş ancak şüphelilerin tespitinde kullanılabilecek herhangi bir maddi delile rastlanılmamıştır.

İşbu rapor 3 (üç) sayfa olarak tanzim edilmiştir. 23.05.2018 saat 15.40.

225613
Polis Memuru

T.C.
İSTANBUL
CUMHURİYET BAŞSAVCILIĞI

20/06/2018

Soruşturma No : 2018/59986

DAİMİ ARAMA KARARI
SİBER SUÇLARLA MÜCADALE ŞUBE MÜDÜRLÜĞÜ'NE

DAVACI	: **K.H.**
MÜŞTEKİ	: KOİNEKS TEKNOLOJİLERİ A.Ş.
VEKİLİ	: AV. BEDİRHAN OĞUZ BAŞIBÜYÜK
ŞÜPHELİ	: Meçhul
SUÇ	: Hırsızlık
SUÇ TARİHİ VE YERİ	: 07/03/2018 İSTANBUL
T. E.K.M	: TCK 142/2-e, 53/1. Maddeleri
ZAMANAŞIMI SÜRESİ	: 15 Yıl
ZAMANAAŞIMI TARİHİ	: 07/03/2033

SORUŞTURMA EVRAKI İNCELENDİ:

Müşteki şirket vekili müşteki şirketin bilişim sistemlerine izinsiz erişim sağlanarak şirket bünyesindeki sanal paraların başka hesaplara yönlendirildiğini belirterek müracaatta bulunması üzerine soruşturma yürütülmüş ise de; Tüm araştırmalara rağmen şüphelilerin tespit edilemediği,

Bu şekilde, atılı suçu işlediği iddia edilen kimliği tespit edilemeyen şüphelinin/şüphelilerin, çok sıkı bir şekilde araştırılarak kimliğinin/kimliklerinin belirlenmesi, yakalandığı/yakalandıkları takdirde mevcutlu olarak savcılığımıza sevk edilmesi/edilmeleri, aksi halde zamanaşımı tarihine kadar sürekli olarak araştırmaya devam edilmesi ve tekide mahal verilmeksizin her üç ayda bir Cumhuriyet Başsavcılığımıza bilgi verilmesi rica olunur.

ÖMÜRHAN DUR 104662
Cumhuriyet Savcısı
e-imzalıdır

ADRES : İstanbul Adalet Sarayı Çağlayan Meydanı Gürsel Mah. No:1 Şişli / İSTANBUL
İRTİBAT : Bilişim Suçları Bürosu - 6 Kat A-1 Blok No:657
TEL : 0 212 375 75 75 Dahili : 55694 **FAKS:** 0 212 375 78 75