OUCH!

SANS SECURITY AWARENESS

Herkes İçin Aylık Güvenlik Farkındalığı Bülteni

CEO Dolandırıcılığı / BEC

CEO Dolandırıcılığı/ BEC Nedir?

Siber saldırganlar CEO dolandırıcılığı ya da Şirket E-posta Anlaşması (BEC) olarak adlandırılan e-posta saldırılarına doğru yönelmeye devam ediyorlar. Bunlar kurbanlarını yapmamaları gereken birsiyi yaptırmak için oyuna getiren nokta atisi seklinde planlanmış e-posta saldırılarıdır. Çoğunlukla kotu adamlar paranın pesindedir. Bu saldırıları tehlikeli yapan şey siber saldırganların kurbanları hakkında sal diriyi yapmadan araştırma yapıyor olmasıdır. Ayrıca e-posta içinde tespit edilebilecek virüs bulaştırılmış bir e-posta eki ya da kotu niyetli bir web bağlantısı olmadığı için, güvenlik teknolojilerinin bu tip saldırıları durdurması çok zordur. Saldırı nasıl gerçekleşiyor ona bakalım.

Siber saldırganlar kurbanları ve kurbanlarının etkileşimde olduğu kişiler ile ilgili araştırma yapmak için interneti kullanırlar. Örneğin eğer size hedef aldılarsa sizin is vereninizin ya da belki birlikte çalıştığınız emlakçının kim olduğunu araştırabilirler. Daha sonra da size sanki bu kişilerden geliyormuşçasına bir e-posta hazırlayıp size gönderirler. Bu e-posta bir faturanın ödenmesi, ödeme yapılacak kişinin değiştirilmesi gibi sizi hemen harekete geçirecek bir aciliyet içerir ya da kritik bilgileri içeren bir cevap vermeye size ikna edecek şekilde. Sizi onların istediği şeyi yaptırmaya zorlayan bir e-postadir bu aslında. Aşağıda bu saldırıların nasıl islediğine dair iki örnek bulabilirisiniz:

Para Transferi: Bir siber saldırgan paranın pesindedir. Muhasebede alacakları kimin ödediğini ya da para transferinin kimin yaptığını belirlemek üzere çalıştığınız şirketi araştırırlar. Daha sonra saldırganlar bu kişilere sanki patronlarından ya da üst düzey yöneticilerinden geliyormuş gibi bir e-posta hazırlar ve gönderirler. Bu e-posta acil bir durum olduğunu ve yeni bir banka hesabına hemen para transferi yapılması gerektiğini bildirir. Onları yanlış yapmaya zorlayarak gerçekte parayı siber suçlulara göndermesini sağlar.

Vergi Dolandırıcılığı: Siber suçlular vergi dolandırıcılığında kullanılmak üzere kişilerin kişisel bilgilerinin pesindedir. Bunun en kolay yollarından biri bir şirketin tüm çalışanlarının bilgilerini çalmaktır. Siber saldırganlar Ihsan Kaynaklarında kimin çalıştığını araştırılar. Daha sonra bu kişilere sanki üst düzey yöneticilerinden ya da bir tüzel kişilikten geliyormuş gibi sahte e-postalar gönderirler. Bur e-posta hemen çalışmaların vergi bilgilerini göndermelerini isteyen acil bir yalan içerir. Ihsan Kaynaklarındaki kişiler bu kritik bilgileri üst düzey yöneticilerine gönderdiklerini düşünürler ama gerçekte bu bilgileri siber suçlara gönderiyorlardır.

Kendinizi Korumanın Yolları

Peki kendinizi nasıl koruyabilirsiniz? Sağduyunuz sizin en iyi korunma yolunuzdur. En yaygın ipuçları aşağıda bulabilirsiniz:

E-posta çok kısadır ve aciliyet içeriyordur. Çoğunlukla birkaç cümleden oluşur ve e-postanın en altında bu postanın mobil bir cihazdan gönderildiğini görürsünüz.

Is yeri kurallarını yok sayarak harekete geçmenizi sağlayacak kadar güçlü bir aciliyet duygusu içerir. E-posta şirket müdüründen ya da patronunuzdan geliyor olsa dahi her zaman işyeri kuralları ve süreçlerini uygulayın.

Bu e-posta isle ilgilidir ancak kişisel bir e-posta adresinden gelmiştir, örneğin @gmail.com ya da @hotmail.com gibi.

E-posta sizin tanıdığınız bir üst düzey bir yönetici, is arkadaşı ya da bir tedarikçiden geliyormuş gibidir ancak e-postayı yazma tarzları onlarınkine benzemez.

Ödeme talimatları bildirilir ve bu talimatlar sizin daha önceden aldığınız talimatlardan farklıdır, örneğin acil bir şekilde farklı bir banka hesabına ödeme yapılması gibi.

Eğer hedef alındığınızdan şüpheleniyorsanız, saldırgan ile tüm iletişiminizi teksin ve yetkilinize hemen bu konu ile ilgili rapor verin. Eğer evde kişisel olarak hedeflenmişseniz ya da kurban olup para transferi yapmışsanız hemen bankanıza ve sonrasında polise bunu bildirin.

Türkçe Çevirisi

Selma Süloğlu, ODTÜ Bilgisayar Mühendisliğinde doktorasını tamamlamış olup Hawaii Üniversitesinde yazılım mimarileri ve yazılım güvenliği üzerinde doktora sonrası araştırma yapmaktadır.

Sema Yüce, Türkiye'nin önde gelen kurumsal şirketlerinde ve özellikle bilişim, finans, telekomünikasyon, sigortacılık, sanayi, perakendecilik gibi sektörlerde; bilgi güvenliği, uyum, BT yönetişim/strateji, risk yönetimi, iş sürekliliği, hizmet yönetimi, altyapı hizmetleri, yazılım geliştirme ve program/proje yönetimi alanlarında yönetici ve danışman olarak 19 yılı aşkın süre görev yaptıktan sonra, Truth ISC (www.truth-isc.uk) adıyla kurduğu Türkiye ve İngiltere'de faaliyet gösteren danışmanlık şirketinde hizmet vermeye devam etmektedir.

Konuk Yazar

Don Cavender, *adli bilişimde ve siber suçlarda 22 yıldan fazla görev yapmış eski bir FBI ajanıdır. Washington DC BEC koordinatörü olarak siber suç isleyen organizasyonları hedef almaktadır. Eğitimler vermekte ve adli bilişimde ve siber soruşturmalar ile ilgili araştırma yapmaktadır. Twitter'da @don_cavender ile ve Linkedin'den https://www.linkedin.com/in/donald-cavender adresini kullanarak kendisine ulaşabilirsiniz.*

Kaynaklar

Sosyal Mühendislik:	https://www.sans.org/u/HE3
Otalamayı Durdurun:	https://www.sans.org/u/HE8
Zararlı Yazılımları Durdurun:	https://www.sans.org/u/HEd
Oturumunuzu Kilitleyin:	https://www.sans.org/u/HEi