Herkes İçin Aylık Güvenlik Farkındalığı Bülteni

Oltalama Saldırılarını Durdurmak

Giriş

E-posta ve mesajlaşma servisleri (Skype, Twitter veya Snapchat gibi) en öncelikle kullandığımız iletişim yöntemleridir. Tüm bu teknolojileri iş hayatımız dışında arkadaşlarımız ve ailemiz ile iletişim halinde olmak için de kullanırız. Dünyadaki pek çok insan bu teknolojilere bağlı olduğu için oltalama adı verilen yöntem siber saldırganların öncelikli saldırı yöntemi haline gelmiştir İş veya ev kullanıcısı olduğunuzdan bağımsız olarak oltalama saldırılarını nasıl fark edeceğinizi ve durduracağınızı öğrenin.

Oltalama nedir?

Oltalama e-posta veya mesajlaşma hizmetlerini kullanarak sizi kandırıp kötü niyetli bir bağlantıyı tıklayarak şifre paylaşmanızı yada enfekte olmuş bir e-posta eklentisini açmanızı sağlayan bir saldırı türüdür. Saldırganlar bu mesajları ikna edici hale getirmek için çok çalışırlar ,aciliyet veya merak gibi duygusal tetikleyicilerinizi harekete geçirirler. Mesajlarınızı tanıdığınız bir kişiden veya sıklık ile kullandığınız güvenilir bir şirketten geliyormuş gibi gösterebilirler. Ya da belki bankanızın logolarını ekleyebilir veya mesajın daha meşru görünmesi için bankanızın e-posta adresinden geliyormuş gibi gösterebilirler. Saldırganlar daha sonra bu mesajları milyonlarca kişiye gönderirler. Tuzaklarına kimlerin düşeceğini bilmezler, tek bildikleri ne kadar çok insana ulaşırlar ise o kadar çok kurbanları olacağıdır.

Kendinizi Koruyun

Genel olarak bir e-postayı veya mesajı açmanız veya okumanız normal bir durumdur. Bir oltalama saldırısının işe yaraması için kötü niyetli kişilerin sizi kandırmak için birşeyler yaptırması gerekir Neyseki bir mesajın saldırı olduğuna dair ip uçları vardır. En yaygın olanları:

- Aşırı derecede aciliyet hissi uyandırır , örneğin banka hesabınızın kapanması yada mahkemeye verileceğiniz konusunda tehdit eder ve iyiliğiniz için sizden acil aksiyon talep eder. Saldırganlar size acele ettirerek hata yapmanızı isterler.
- İş yerinizdeki politika ve süreçleri uygulamamanız için baskı yaparlar
- Güçlü bir merak duygusu uyandırır veya gerçek olamayacak kadar iyidir (Hayır, piyango kazanmadınız).
- “Değerli Müşterimiz” gibi genel bir hitap içerir. Oysa ki sizin ile iletişim kuran şirketler yada arkadaşlarınız adınızı bilirler.
- Kredi kartı numaranız, parolanız veya meşru göndericinin bilmesi gereken diğer bilgiler gibi son derece hassas bilgi isterler.

- Mesaj resmi bir kuruluştan geliyor gibi görünür, ancak yetersiz dilbilgisi hataları , yazım hataları içerir veya @ gmail.com gibi kişisel bir e-posta adresini kullanır.
- Mesaj resmi bir e-postadan (patronunuz gibi) gelir, ancak yanıt verildiğinde başka birisinin kişisel e-posta hesabına gider.
- Bildiğiniz birinden gelen bir mesaj gibidir, ne var ki üslup veya kelime seçimi o kişiye aitmiş gibi görünmez. Şüpheleniyorsanız, gönderdiğini düşündüğünüz kişiyi doğrulamak için arayın. Bir siber saldırganın arkadaşınız veya birlikte çalıştığınız bir kişiden geliyormuş gibi görünen bir mesaj oluşturması kolaydır.

Sonunda sağduyu, en iyi savunmanızdır. Bir e-posta veya mesaj garip, şüpheli veya gerçek olamayacak kadar iyi görünüyorsa, bu bir kimlik avı saldırısı olabilir.

Türkçe Çevirisi

Selma Süloğlu, ODTÜ Bilgisayar Mühendisliğinde doktorasını tamamlamış olup SOSoft Bilişim Teknolojilerinde biyometrik güvenlik sistemleri üzerinde çalışmaktadır.

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 Editor

Tonia Dudley 2011 yılından bu yana ödül kazanan oltalama eğitimleri de dahil olmak üzere güvenlik farkındalığı programları yürütmekte ve geliştirmektedir. Kendisine www.linkedin.com/in/toniadudley adresinden ulaşabilirsiniz.

Kaynaklar

Sosyal Mühendislik:	https://www.sans.org/u/Cb1
Başkalarının Güvenli Hale Gelmesine Yardım Etmek:	https://www.sans.org/u/Cb6
E-posta için Yapılması ve Yapılmaması Gerekenler:	https://www.sans.org/u/Cbg
CEO Dolandırıcılığı:	https://www.sans.org/u/Cbl
OUCH! Çevirileri ve Arşiv:	https://www.sans.org/u/Cbq

Lisans