Bilgisayar Kullanıcıları için Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...

Oltalama

Genel Bakış

E-posta temel iletişim yöntemlerimizden birisidir. Her gün sadece iş için değil, aynı zamanda ailelerimiz ve arkadaşlarımızla iletişimde kalmak için de kullanırız. Ayrıca e-postalar artık birçok şirketin satın alma onayınızı ya da banka hesap özetlerinizi iletmek gibi çevrimiçi hizmetlerini sunma aracıdır. Dünyada e-postalara bağlı bu kadar çok insan olunca, siber suçlular için de temel saldırı yöntemi haline geldi. Bu bültende size yaygın bir e-posta ile saldırı yöntemi olan "oltalama"yı ve e-postayı güvenle kullanmak için atabileceğiniz adımları anlatacağız.

Konuk Yazar

Dr. Lance Hayden Berkeley Araştırma Grubu'nun Yönetici Direktörüdür. Güvenlik kültürü ve davranışları alanlarında uzman olduğu gibi, McGraw-Hill yayınlarından çıkan People-Centric Security: Transforming Your Enterprise Security Culture kitabının yazarıdır. Kendisine www.linkedin.com/in/drhayden bağlantısından ulaşabilirsiniz.

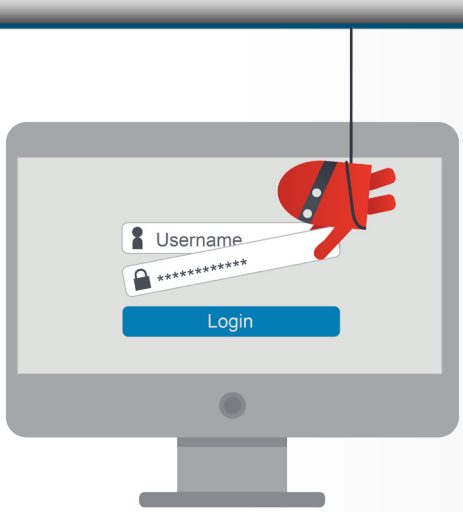
Oltalama

Oltalama e-posta ya da mesajlaşma servislerini kullanarak sizin örneğin bir sosyal medya sitesinde bir aksiyon almanızı, bir bağlantıyı tıklamanızı ya da bir ekli dosyayı açmanızı sağlayarak sizi kandıran bir saldırı türüdür. Böyle bir saldırının kurbanı olarak riskiniz hassas bilgilerinizin çalınması ya da bilgisayarınızın ele geçirilmesi olabilir. Saldırganlar oltalama e-postalarının ikna edici olması için gerçekten çok çalışıyorlar. E-postalarını sizin tanıdığınız biri ya da bildiğiniz bir yerden, örneğin bir arkadaş ya da sıkça kullandığınız güvenilir bir şirketten geliyormuş gibi gösteriyorlar. Hatta bankanızın logolarını ekleyip, mesajın gerçekliğine sizi inandırabilmek için e-posta adreslerini onlarınkine benzetiyorlar. Sonra bu oltalama e-postalarını milyonlarca insana gönderiyorlar. Kimin tuzağa düşeceğini bilmiyorlar, tek bildikleri ne kadar çok gönderirlerse, başarma şanslarının o kadar yüksek olduğu. Oltalama bir ağ ile balık yakalamaya çalışmaya benzer, ne yakalayacağınızı bilemezsiniz ama ağınız ne kadar büyükse, daha fazla balık yakalama şansınız daha yüksektir. Oltalama ile istediklerini elde edebilmek için saldırganların kullandıkları temel birkaç yöntem var:

- **Bilgi Toplama**: Saldırganın amacı parolalarınız, kredi kartı ya da bankacılık bilgileriniz gibi kişisel bilgilerinizi ele geçirmektir. Bunu yapmak için size içeriğinde bilinen ve orjinal görünen bir siteye yönlendirme bağlantısı bulunan bir e-posta gönderir. Bu site sizden kişisel bilgilerinizi ya da hesap bilgilerinizi ister. Ne yazıkki bu site sahtedir ve verdiğiniz herhangi bir bilgi doğrudan saldırgana gider.
- **Kötü Niyetli Bağlantılar**: Saldırganın amacı cihazınızı kontrol altına almaktır. Bunu yapmak için size bir bağlantı içeren e-posta gönderir. Eğer bağlantıyı tıklarsanız, cihazınıza yönelik saldırı başlatan ve başarılı olursa sisteminizi ele geçiren bir siteye yönlendirilirsiniz.

Oltalama

- **Kötü Niyetli Dosya Ekleri**: Saldırganın amacı aynıdır, cihazınızı ele geçirmek. Ancak bir bağlantı göndermek yerine, size Word dokümanı gibi kötü niyetli bir dosya eki gönderir. Eki açmak, saldırıyı başlatır ve sisteminizi muhtemelen saldırganın ele geçirmesine yol açar.
- **Aldatmacalar**: Bazı saldırganlar dijital hayata geçiş yapan dolandırıcılardan başka birileri değildir. Sizi bir piyango kazandığınızı söylerek, hayırsever bir kurum gibi yardım isteyerek ya da milyonlarca doların transferine yardımcı olmanızı isteyerek kandırmaya çalışırlar.Eğer herhangi birine yanıt verirseniz, paranızı alabilmek için sizden öncelikle hizmetleri için bir ödeme ya da banka hesap bilgilerinize erişim talep edeceklerdir.



En güçlü savunmanız sağduyunuzdur. Eğer bir e-posta ya da mesaj garip, şüpheli ya da gerçek olamayacak kadar iyi görünüyorsa, bu bir oltalama saldırısı olabilir.

Kendinizi Korumak

Hemen hemen tüm olaylarda, bir e-postayı açmak ve okumakla ilgili bir sıkıntı yoktur. Bir oltalama saldırısının çalışması için saldırganların sizi birşeyler yapmak üzere kandırması gerekir. Neyse ki, bir e-postanın saldırı olup olmadığını anlamak için bazı ipuçları vardır, en yaygın olanlarını şöyle sıralayabiliriz:

- E-posta aciliyet hissi uyandırır, kötü birşeyler (banka hesabınızın kapatılması gibi) olmadan önce acil aksiyon almanızı ister. Saldırgan, size düşünmeden hata yapmaya zorlamak istiyordur.
- Beklemediğiniz bir dosya içeren bir e-posta alırsınız ya da e-posta size ekli dosyayı açmak için kandırmaya çalışıyordur. Henüz duyurulmamış işten çıkarmalar listesi, çalışan maaş artış bilgileri ya da hakkınızda bir dava açıldığını belirten ekler bunlara örnek olabilir.
- Sizin adınızı kullanmak yerine “Değerli Müşterimiz” gibi daha genel ifadeler kullanılır. Birçok firma ya da arkadaşlarınızın birçoğu adınızı bilir.
- Böyle e-postalar sizden kredi kartı numaranız ya da parolanız gibi yüksek hassasiyetli bilgiler ister.
- E-posta size resmi bir kurumdan geldiğini söylüyordur, ancak yazım dili hatalarla doludur ya da gönderen e-posta adresi @gmail.com, @yahoo.com, ya da @hotmail.com gibi kişisel bir hesaptır.
- Bağlantılar gariptir ya da olması gereken adresler değildir. İpucu, bağlantının üzerine gelip, gerçekte size hangi bağlantıya yönlendireceğini görerek, karar vermenizdir. Eğer görünen bağlantı ismi ile gerçekte size yönlendireceği bağlantı aynı değilse, sakın tıklamayın. Mobil cihazlarınızda bir bağlantının üzerinde parmağınızı aşağıya doğru kaydırarak bu bilgiyi görebilirsiniz. Hatta daha güvenli bir yöntem, e-postanızdaki bağlantı adresini kopyalayıp, internet tarayıcınıza yapıştırmak ya da doğru bağlantıyı yazmaktır.
- Mesaj bildiğiniz birisinden geliyordur, ancak tarz, kullandığı kelimeler ondan farklıdır. Eğer şüpheleniyorsanız, gönderen

Oltalama

kişiyi arayıp doğrulayın. Bir siber saldırgan için kişisel ya da iş arkadaşınızdan geliyormuş gibi görünen bir e-posta oluşturmak çok kolaydır.

Eğer bir e-postanın ya da mesajın oltalama saldırısı olduğuna inanıyorsanız, basitçe silin. Sağduyunuz kesinlikle en güçlü savunmanızdır.

Daha Fazla Bilgi İçin

Aylık OUCH! güvenlik farkındalığı bültenine üye olun, OUCH! arşivlerine erişin ve http://www.securingthehuman.org adresini ziyaret ederek SANS güvenlik farkındalığı çözümleri hakkında daha fazla bilgi edinin.

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, telekomünikasyon, sanayi, perakendecilik gibi sektörlerde; bilgi güvenliği, iş sürekliliği, risk yönetimi, altyapı hizmetleri, yazılım geliştirme ve proje yönetimi alanlarında yönetici ve danışman olarak 15 yılı aşkın süredir görev yapmaktadır.

Mustafa Emrah Ünsür, Güvenlik Araştırmacısı olarak araştırmaları, makaleleri ve çevirileri vardır. Beyaz Şapkalı Hacker olarak kendisi tarafından kodlanan ve kodlanmakta olan 'exploit'ler ve 'tool'lar bulunmaktadır. Ayrıca, Sızma Testi Uzmanı olarak özel şirketlere ve devlet kurumlarına Zafiyet ve Sızma Testi yapmış ve yapmaya devam etmektedir.

Kaynaklar

Sosyal Mühendislik:	https://www.securingthehuman.org/ouch/2014#november2014
Güvende Olmak için 5 Adım:	https://www.securingthehuman.org/ouch/2014#october2014
Ele Geçirildim, Şimdi Ne Olacak?:	https://www.securingthehuman.org/ouch/2014#may2014
OnGuard Online:	https://www.onguardonline.gov/phishing
SANS Günün Güvenlik İpucu:	https://www.sans.org/tip_of_the_day.php

Yayın Kurulu : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis