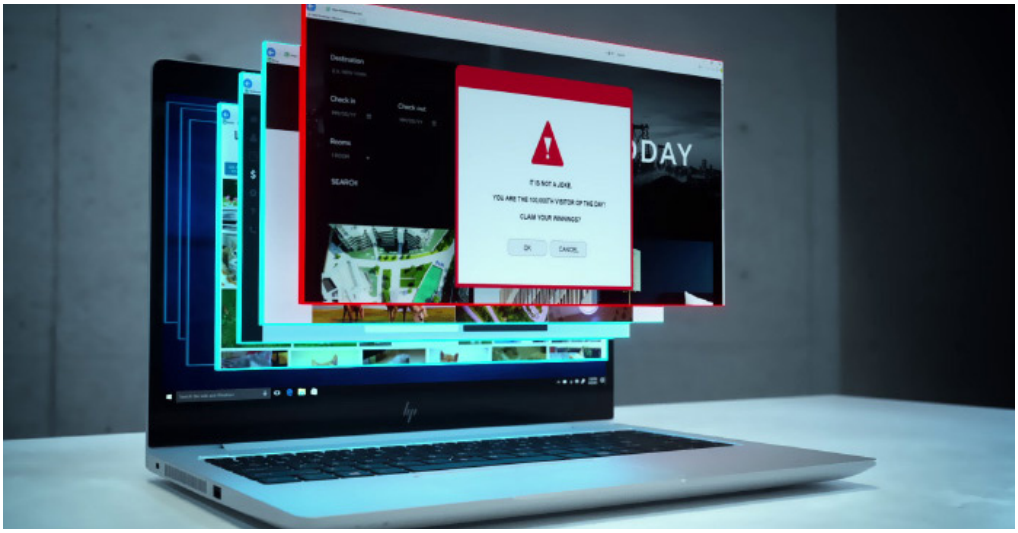
Kimlik avı artık sadece e-postalar için değil

Emre Gursoy tarafından yazıldı

Ayrintili bilgi edinin



Bir web tarayıcısı, hem bir bilgi dünyasına hem de tehditlere giden bir giriş kapısı sağlıyor. Bu durumda, işinizi korumak için bu konuyla ilgili ne yapabilirsiniz?

Web tarayıcılarının cevaplayacağı çok şey var. Yakın zamanda 400 CIO arasında yapılan bir ankette, katılımcıların %68'i siber suçların çok gelişmiş olduğunu, çalışanların güvenli ve güvenli olmayan siteleri ayırt etmede güçlük çektiklerini söyledi[1]. Bu durum düşünüldüğünde, BT uzmanlarının %70'inin her hafta kimlik avı yaşamalarına ve bunun yalnızca e-posta aracılığıyla olmadığına şaşırmamak gerek[2]. Üst düzey hacker'lar çalışanları hassas kişisel bilgilerini açıklamaya ikna etmek için artık sosyal medya, reklam ve yaygın olarak kullanılan web sitelerindeki yazım hatalarını kullanıyor. Kimlik avı dolandırıcılıklarının tanınması gittikçe zorlaştıkça, işletmeler kendi iş gücünü bu saldırılardan korumak için mücadele ediyor.

Güvenlik yazılımı ve çalışan eğitimi konusunda daha fazla farkındalık ve yatırım olmasına rağmen, son altı yıldır dizüstü ve masaüstü bilgisayarlara yapılan siber saldırılarda %232'lik bir sıçrama oldu[3]. Siber suçlular saldırılarına devam ediyor çünkü rakamlar onları destekliyor. Verileri korumak için muazzam bir çaba harcanır, ancak işinizi yıkmak için yalnızca bir çalışanın kötü amaçlı bir bağlantıya tıklaması yeterlidir.

Sosyal medya siber saldırıları bu sorunun büyük bir parçasıdır. Facebook ve Twitter gibi platformlar siber suçlar için zengin av alanlarıdır. Bu platformlar bağlantı ve iletişim amacı taşımalarının yanı sıra kullanımı kolay ve işletilmeleri ucuzdur. Sahte hesaplar açıp bağlantılardan kötü amaçlı içerik göndermeye başlamak, güvenilmez açılır pencereler (pop-up) yoluyla karşılama sayfalarına veri harmanlamak son derece kolaydır.

Bu çevrimiçi etkinliklerin çoğunluğu, önceden e-postaya yönelik olarak kullanılan kimlik avı tekniklerine dayanmaktadır. Sosyal medya insanlar arasında bağlantılar sağlar ve gerçek, inandırıcı bir kimlik oluşturup platformların gerçek kullanıcılarını takip etmek çok da zor değildir.

Video akış hizmeti Vevo yoğun veri ihlalinin en son kurbanıydı. Bir çalışanı LinkedIn kimlik avı dolandırıcılığında hedef alındı ve 3,12 TB dâhili dosya çevrimiçi olarak sızdırıldı. Bu dosyalar videoları, ofis belgelerini, promosyon materyallerini, ileride kullanılacak olan sosyal medya içeriklerini ve Vevo ile işbirliği yapan plak şirketleri ile anlaşması bulunan plak sanatçılarının bilgilerini içeriyordu[4].

Hack ekibi OurMine, bir Vevo çalışanı ile e-posta üzerinden yapılan bir münakaşadan sonra saldırının sorumluluğunu üstlendi. Bu durum belirli bir hedeften belirli ayrıntıları çalmaya çalışan hedefe yönlendirilmiş bir saldırı olan **spear-phishing** (mızrak avı) tehlikesidir. Hacker'ların en sık uyguladığı yöntem, hedef aldıkları kişiyi bilgi vermeye ikna etmek için kendilerini arkadaş ya da güvenilir bir kaynak (ör. bankanız) olarak göstermektir ki bu eylem, saldırıların %91'ini oluşturmaktadır.

Kimlik avı artık sadece e-postalar için değil

Vevo gibi kimlik avı saldırılarının kurbanı olan birçok işletme için sonuçlar hem hasar verici hem de uzun süreli olabilir. Bu saldırıların sonucunda çalışan verimliliği ve müşteri verilerini kaybetme ihtimalinin yanında, müşterilerin kendilerini de kaybedebilirler. İşinizde müşterilerinizin güveni, güvenlik ihlali nedeniyle büyük bir darbe alabilir, onlar için artık güvenilir bilgi sahibi olmazsınız. Bunun üstesinden gelinebilse de sonuçlar genellikle kalıcı olur.

Öyle ki 2017 yılının 4. çeyreğinde sosyal medya kimlik avı saldırıları, kendini büyük isme sahip markaların müşteri desteği olarak tanıtan sahte hesaplara olan eğilim ile %500'e sıçradı[5]. Bu gelişme angler-phishing (olta avı) olarak bilinmeye başladı çünkü saldırganlar yem atıp sosyal medya kullanıcılarının onlara gelmelerini bekliyordu. Web tabanlı sosyal medyaya güvenen milyonlarca insan, aynı markayı ve gerçek gibi görünün hesap adını kullanan ikna edici bir saldırıyla sık sık aldatıldı. Ardından, kullanıcılar bağlantı kurar kurmaz sahte hesap onlara kimlik avı sitesinin bağlantısını göndererek oturum açmalarını istedi. Bu da kimlik avcısının esas hedefi olan özel verileri elde etmesini sağladı.

Çalışanlarınızın sosyal medya üzerinden kimlik avcılarına yakalanmasını önlemenin en kolay yollarından biri, iş yerinde davranış değişikliğini teşvik etmektir. Bunu yapmak çalışanlarınızın, işiniz için yıkıcı sonuçlara yol açacak basit hatalardan kaçınmalarına yardımcı olur:

1. Etkileşimleri güvenebileceğiniz kullanıcılarla sınırlayın
2. Doğrulanmayan kaynaklardan gelen bağlantılara tıklamayın
3. Sosyal medyadan asla dosya ekleri indirmeyin
4. Tüm sosyal medya hesapları ve cihazlarında iki faktörlü doğrulamayı etkin hale getirin, bu şekilde saldırıya uğramaları zorlaşacaktır
5. Yüksek erişim ayrıcalıkları olan veya sosyal ortamda bireylerle yüz yüze gelen çalışanlara ilave eğitim verin

Siber anlamda dirençli kalabilmek için kullandığınız teknoloji, güvenlik planınızın dikkat etmeniz gereken diğer bir vazgeçilmez yönüdür. Örneğin HP Elite ailesi, baştan aşağıya güvenlikle tasarlanmış dizüstü ve masaüstü bilgisayarlardır.

Bu özelliklerden biri, güvenli taramaya farklı şekilde yaklaşan HP Sure Click özelliğidir ve HP Elite platformlarında bulunmaktadır. Yalnızca kullanıcıların kaçınması gereken tehlikeleri sitelere bayrak eklemek yerine, aynı zamanda diğer tarayıcı sekmeleri ve daha geniş sistemlerden kötü amaçlı yazılım, fidye yazılımı ve virüslerin bulaşmasını önler. Bir kullanıcı tarama oturumunu başlattığında, ziyaret edilen her site HP Sure Click'i tetikler. Örneğin, bir web sitesi her ziyaret edildiğinde, HP Sure Click donanım tabanlı ayrı bir tarama oturumu başlatır ve bu oturum, bir web sitesinin diğer sekmelere veya sistemin kendisine bulaştırma becerisini ortadan kaldırır.

Konu işletmelerin güvenlik stratejilerini değiştirmelerine ve HP EliteBook 800 Serisi (isteğe bağlı 8. Nesil Intel® Core™ İşlemcileri içerir) gibi en son teknoloji ürünü cihazlara ayak uydurmaya geldiği zaman, söylemek yapmaktan daha kolaydır. HP Hizmet Olarak Cihaz (DaaS) çözümü bu noktada devreye girer. Ticari kuruluşların çalışanlarını doğru donanım ve aksesuarlarla donatma, çoklu işletim sistemi filolarını yönetme ve ek yaşam döngüsü hizmetlerini sağlama yollarını basitleştiren modern bir PC tüketim modelidir. HP DaaS, her şeyin sorunsuz ve etkili şekilde çalışması için basit fakat esnek planları cihaz başına tek fiyatla sunar.

Sonuç olarak, iyi eğitimli bir ekip ve güvenlik için optimize edilmiş cihazlara sahip olmak, en büyük siber tehditlerden biri olan sosyal medya siber suçlarıyla mücadele etmenize yardımcı olur. Zamanla bu tehditler daha da büyük ve daha kötü niyetli hale gelecek, o nedenle savunmalarınızı güçlendirmenin şimdi tam zamanı.

Şirket cihazlarınızı nasıl koruyacağınız konusunda daha fazla bilgi edinmek için, ve HP güvenlik çözümlerini işinize olan faydalarını keşfedin.

Kaynaklar:

1. https://www.bromium.com/company/press-releases/majority-cios-believe-they-are-losing-battle-against-cybercrime.html
2. https://www.engineering.com/DesignerEdge/DesignerEdgeArticles/ArticleID/8355/HP-Nearly-70-of-IT-Professionals-Experience-Weekly-Phishing-Attacks.aspx
3. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/
4. https://www.zerofox.com/blog/vevo-hacked-via-linkedin-phishing-campaign/
5. https://www.infosecurity-magazine.com/news/social-media-phishing-attacks-soar/

4AA7-3218TRE, Mayıs 2018