COMODO
Creating Trust Online®

COMODO UYARIYOR:
KAPIDAN DEĞİL BİLGİSAYARINIZDAN GİREN HIRSIZLARA DİKKAT

Evlere artık e-mail ile giren sanal hırsızlar, phishing adı verilen yöntemle hedef kişilerin banka, kredi kartı veya sanal hesaplarına dair bilgilerini ele geçiriyor. Bu şekilde işlenen siber suçların toplam maliyetinin 500 milyar doları bulduğu tahmin ediliyor.

Bugüne kadar NASA, New York Borsası ve ABD Başkanı Barack Obama'nın siber güvenliğini sağlayan, dünyanın önde gelen siber güvenlik firmalarından biri olan COMODO'nun Mühendislik Başkan Yardımcısı Egemen Taş, phishing hakkında merak edilenleri yanıtladı:

Dolandırıcılıkta phishing yöntemi nedir?

Phishing "Password" (şifre) ve "Fishing" (balık avlamak) sözcüklerinin birleştirilmesiyle oluşturulan ve Türkçe'ye oltalama (yemleme) saldırısı olarak çevrilebilecek bir internet saldırı çeşididir. Bu yöntem genelde sanal dolandırıcılar tarafından gönderilen mail veya oluşturulan web sayfası yoluyla gerçekleştirilmektedir. "Kimlik avı" tabiri ile de anılan bu yöntemde, kullanıcıya gönderilen e-postaya bilinen bir kişi veya kurumdan gelmiş izlenimi verilmekte ve kullanıcıda acil bir durumun, bir fırsat veya tehdidin oluştuğu izlenimi yaratılarak ani bir karar ile dikkatsiz hareket etmesine çalışılmaktadır. Bu şekilde davranan kullanıcıdan kimlik bilgileri, kredi kartı / banka hesap bilgileri, kullanıcı şifre bilgileri istenmekte; kullanıcı bu bilgileri aslına çok benzeyen sahte form ve web sitelerine girdiği anda bu bilgilerin çalınması veya zararlı bir yazılımın bilgisayarına indirilmesi hedeflenmektedir.

Örneğin "Garanti Bankası" adı kullanılarak gönderilen epostanın içeriğinde kullanıcının kullanıcı-adı ve şifresinin elde edilmesi hedeflenirken, "Turkcell Fatura" adı kullanılarak gönderilen e-posta "fatura.exe" adlı bir zararlı yazılımın bilgisayara indirilmesi isteniyor olabilir. Bu zararlıyı indirip bilgisayarına kuran kişi, çok ciddi anlamda sıkıntı yaşayıp, tüm dosyalarını kaybetme, verilerin dışarıya sızdırılması veya tüm iletişiminin kötü niyetli kişilerce izlenebilmesine yol açabilecek tehlikelerle karşı karşıya kalabilmektedir. Kurumsal firmalara yönelik geliştirilen özel saldırı çeşitlerinde (hedefli oltalamada [spear

phishing]) amaç genelde kurumsal varlıklara odaklanıp, örneğin kredi kartı veritabanı, veya müşteri veritabanının dışarıya sızdırılmasıdır.

Benzer şekilde, web'de gezinen herhangi bir kullanıcı, gerçek izlenimi veren sahte bir web sitesine denk gelip, burada oltalama saldırısıyla karşılaşabilir. Yine benzer hedeflere yönelik geliştirilen sahte web siteleri kullanıcılar açısından bilgi/belge ve hesapların ele geçirilmesi için kullanılmaktadır.

Kaç tür olta dolandırıcılık yöntemi vardır?

Teknik olarak bakıldığında onlarca farklı yöntemden bahsetmek mümkündür. Bunların arasında aldatıcı, zararlı yazılım kökenli, klavye kaydedici, arka kapı, DNS-bazlı, MITM, oturum çalma yöntemleri en çok kullanılanlardır. Neredeyse zararlı yazılım çeşidi sayısı kadar oltalama yöntemi vardır.

Fakat amaç açısından bakıldığında temelde iki farklı yöntemden bahsetmek mümkündür. Birinci yöntemde amaç kullanıcının değerli bir verisinin kötü niyetli kişilerce ele geçirilmeye çalışılması (verinin dışarıya kaçırılması), ikincisinde ise zararlı bir yazılım/kod parçası kullanıcının bilgisayarına sızdırılmaya çalışılmasıdır (zararlıyı içeriye sızdırılması). Zararlı yazılım bilgisayara bulaştığında yol açabileceği hasarlar bireysel düzeyde olabileceği gibi, büyük bir şirketin en değerli varlıklarını da hedef alabilir. Bu zararlı yazılımlar genelde belgelerin çalınması için, bozulması için veya şifrelenip fidye amacıyla kullanılması için oluşturulmaktadır.

Bunlardan birkaçını örnek olarak verebilir misiniz?

Son yıllarda Türkiye'de sıkça karşılaştığımız ve hala da farklı şekillerde karşımıza çıkan en güncel örnekler "PTT Fatura", "Türk Telekom Fatura" veya "Turkcell fatura" oltalama e-postalarıdır. Bu e-postalar ile ülke çapında bilinirliği yüksek markalar kullanılarak kullanıcılar aldatılmakta ve fatura ödeme sayfasına yönlendirilerek zararlı dosyaların bilgisayara indirilmesi sağlanmaktadır. Bu zararlı dosyayı çalıştırdığınız anda bilgisayarda tüm belgelerin şifrelenerek ulaşılması imkansız hale gelmekte ve bunların açılması karşılığında fidye talep edilmektedir.

Diğer bir hedef kitle de banka müşterileridir. Örneğin dünyada birçok ülkede şubesi bulunan HSBC, Western Union gibi kuruluşlar veya PayPal gibi internet üzerinden para alışverişinde kullanılan sitelere erişim için kullanıcı bilgileri çalınmaktadır.

Dünyanın önde gelen firmalarından HomeDepot, Target, Sony Pictures gibi firmalara yapılan saldırılar ile milyonlarca kredi kartı bilgisi ve şirketlerin gigabyte'larca mahrem bilgileri çalındı. Bu saldırıların başlangıç noktası, genelde basit bir email'in güvenlik sistemlerini geçip şirketin bir çalışanının posta kutusuna düşmesi ve bu çalışanın dikkatsizce o linke tıklayarak bir zararlıyı bilgisayarına indirmesiyle başlamaktadır. Saldırıyı gerçekleştirmek için harcanan çaba ile verdiği zarar arasında inanılmaz bir boyut farkı vardır.

Son dönemde operatör gibi düzenlenmiş sahte mailler rövanşta. Bu yöntemle ne tür bilgiler ele geçiriliyor?

Operatör, sistem yöneticisi veya yetkili kişilerce düzenlenmiş gibi görünen e-postalar ile çoğunlukla kişilerin kullanıcı adı ve şifre bilgileri ele geçirilmeye çalışılmaktadır. Şifre yenileme, kotanın dolması, zaman aşımı gibi acil harekete geçilmesini gerektirecek bir durum oluşturulan oltalama yöntemlerinde amaç kullanıcıyı dikkatsiz yakalamak ve bu bilgileri elde etmektir.

Ayrıca vatandaşlar bu tip dolandırıcılıklardan korunmak için ne yapabilir?

Temel kural: Bu konuda alınacak ilk önlem kişilerin bilmedikleri herhangi bir elektronik posta ekini veya linki açmamaları olur. Kullanıcıların şifre, banka kartı, kişisel bilgi vb. bilgileri e-posta ile yönlendirilen sayfalara kesinlikle vermemeleri gerekiyor. Hiçbir banka ya da büyük kuruluş kullanıcının kişisel bilgilerini mail yoluyla talep etmez. Kullanıcıların en başta bunu bilmeleri gerekir.

Bunun dışında, e-posta sunucu güvenliğini sağlamaları için mutlaka bu amaçla üretilmiş siber güvenlik çözümlerinden faydalanmaları gerekir. Güncel siber güvenlik uygulamaları kullanmaları ve her durumda güncel bir zararlı yazılım koruma programı gerekmektedir. Her ne kadar bilinen zararlı yazılımlar ve saldırılardan mevcut programlar ile koruma yöntemleri geliştirilse de, bilinmeyen yeni zararlı yazılımların bilgisayara sızması %100 engellenememektedir. Daha aktif bir koruma için güncel anti-virüs yazılımları ile birlikte yeni çıkan ataklara karşı davranışsal analiz ve zararlı yazılım analizini online olarak yapabilecek yazılımlar kullanmaları çok önemlidir. COMODO'nun "containment (önleme)" teknolojisi bu amaçla geliştirilmiştir. Bu teknolojiyi içeren kurumsal ve bireysel ürünler, bu tür zararlı yazılımların tespiti ve önlenmesi konusunda "sıfırıncı gün koruması ve virüssüzlük garantisi verebilen tek çözüm" olarak tüm dünyada hızla kullanıcı sayısını artırmaktadır.

Eğer bu tuzağa düştülerse sadece şifre değiştirmekle bundan kurtulabilirler mi?

Kimlik ve şifre hırsızlığı durumu oluşursa yapılacak ilk iş şifrelerin sıfırlanması olacaktır. Fakat ne yazık ki bu da tek başına yeterli değildir. Kullanıcıların verilerinin yedeklerini alması ve hesaba giriş yaparken ikinci bir onaylama ve doğrulama yöntemi kullanılması çok faydalı olacaktır. Örneğin kullanıcı adı ve şifrenizi girdikten sonra SMS ile gelen ikinci bir şifreye ihtiyacınızın olması gibi.

İletişim:
Banu Buyurgan

GTC İletişim Danışmanlığı
+90 312 447 00 20

banu.buyurgan@gtc.com