GÜVENLİ GÜNLER BÜLTENİ

ŞUBAT 2016

Bilgisayar kullanıcılarına yönelik hazırlanır. Her ayın 15'i çıkar. Bültenlerin her ay size ulaşması için üye olunuz: http://eepurl.com/bP-tWn

Oltalama Saldırıları (Phishing)

PHISHING (OLTALAMA) KAVRAMI, İLK OLARAK EPOSTA ARACILIĞI İLE BİLGİSAYAR KULLANICILARINI KANDIRIP, ONLARIN PAROLASINI (PASSWORD) ÇALAN SALDIRI YÖNTEMİ İLE HAYATIMIZA GİRDİ. Bu ilk saldırılarda özel hazırlanmış eposta, sizi parola hırsızlığı yapılmak istenen web sitesine görüntü olarak çok benzeyen, ancak saldırganlar tarafından yaratılmış sahte web sitesine yönlendiriyordu. Bu sahte web sitesine kullanıcı adı ve parola yazıldığında, gizli bilgiler saldırganların eline geçmiş oluyordu.

Ancak, yıllar içinde saldırılar çeşitlendi, parola çalmanın yanında, bilgisayara bir program yükletme (genellikle virüsler), bilgisayardaki bazı dosyaların saldırganlara gönderilmesi (bilgi hırsızlığı) ve benzeri yöntemler için de oltalama saldırıları kullanılmaya başlandı.

Bir başka yazıda detaylandıracağımız hedef odaklı oltalama saldırıları (spear phising) bir kuruma yönelik gerçekleştirilen gelişmiş hedef odaklı siber tehditler (APT – advanced persistent threaat) de oltalama saldırılarından türemiştir.

1 Nedir?

Oltalama saldırıları, kullanıcıların saflığını ve dikkatsizliğini kötüye kullanarak kandırmak ve zarar vermek için yapılan saldırılardır.

Bu saldırıların hedefleri:

1. Kurbana ait gizli bilgileri öğrenmek (örneğin kullanıcı adı, parola)
2. Kurbanın bilgisayarına kötü niyetli yazılım (virüs) yüklemek
3. Kurbanın bilgisayarını uzaktan yönetebilmek (ve bu bilgisayar üzerinden ağa sızmak)
4. Kurbanın bilgisayarı üzerinden ortamı dinlemek (mikrofon), ortamı izlemek (kamera)

2 Bileşenleri

Oltalama saldırıları gerçekleştirilirken, saldırganlar, kurbana yönelik aşağıdaki bileşenleri kullanırlar.

2.1 EPOSTA

Kurbanı ilk kandıran, ona istenmeden yollanan (SPAM) bir epostadır. Bu eposta, görüntü ve içerik olarak, kurbanın güvendiği bir kişi ya da kurumdan geliyor gibi görünür. Özellikle bankalar ve telekomünikasyon şirketleri ile sıklıkla hayatımızda olan havacılık şirketleri ve bazı devlet kurumlarından geliyormuş gibi gözüken epostalar tercih ediliyor. Bunun yanında, daha önce kurban olmuş bireylerin arkadaş çevresine de benzer epostalar gönderiliyor.

Bu epostanın amacı, kurbanda güven sağlayıp, ya eposta ekinde gelen bir dosyayı açtırmak, ya da epostanın içinde bulunan bir sekmeye (link) tıklatmaktır.

2.2 EK

Otlama epostası içindeki ekler genellikle ilk bakışta PDF, TXT ve benzeri uzantılı dosyalar gibi gözükse de içinde kötü niyetli programlar bulunur. Bu dosyaların açılması, kullanıcı onayıyla ilgili programın bilgisayarda çalışması sonucunu doğurur.

2.3 SEKME

Mesaj üzerindeki sekmeler (linkler) epostanın gönderildiği güvenilir kuruma aitmiş gibi gözükür. Bu sekmelere tıklandığında ya kurban saldırgana ait web sitesine gider, ya da Internet'ten, eklerde olduğu gibi, kötü niyetli bir yazılımı bilgisayara indirerek çalıştırır. Örnek olarak, son dönemde büyük zararlara yol açan fidye için dosyaları şifreleyen virüs (cryptolocker) bu yöntemle yayılır.

2.4 WEB SİTESİ

Gerçek siteye görüntü ve içerik olarak çok benzeyen hatta bazı durumlarda tıpatıp aynı görünümlü olacak şekilde yaratılan web siteleri (ya da sadece bir web sayfası), kurbanı değerli bilgileri girmeye yönlendirir. İstenenler genellikle kullanıcı adı, parola, gizli kelimeler, hesap numarası, telefona gelen kısa mesaj (SMS) gibi bilgilerdir. Bu bilgileri direk saldırgana ulaşır ve saldırı tamamlanmış olur.

3 Oltalama (Phishing) Saldırılarına Karşı Dikkat Edilmesi Gerekli 8 Nokta

Oltalama saldırılarından korunmak için dikkat edilmesi gerekenler:

1. Adresi baştan yazın

Eposta içindeki sekmeye (link'e) tıklamayın. Hangi kurumu ziyaret etmek istiyorsanız bu kurumun adresini kendiniz elle yazın.

2. Göndereni doğrulayın

Size beklemediğiniz bir eposta ve ek gönderildiğinde bu kişiye farklı bir yoldan ulaşıp bu mesajın kendisinden gelip gelmediğini doğrulayın.

3. Çevrimiçi görüntüleyici kullanın

Size gönderilen dosyaları (örneğin ofis dosyaları) bilgisayarınıza indirip açmak yerine Google Docs, Office365 gibi çevrimiçi dosya hizmetlerinden birine yükleyip oradan görüntüleyin.

4. Çevrimiçi dosya paylaşımı kullanın

Sık dosya paylaştığınız kişilerle dosyaları, eposta yerine Google Docs, OneDrive, Dropbox gibi bir dosya paylaşım servisi kullanarak paylaşın.

5. Talimatları şüpheyle karşılayın

Size eposta ile gönderilmiş, hassas bilgi isteyen ya da örnek olarak, uzaktan bilgisayara bağlanıp destek verebilmek için bazı bilgileri girmenizi isteyen talimatları şüpheyle karşılayın.

6. Birden çok eposta adresi kullanın

Oltalama saldırılarının size ulaşabilmesi için eposta adresinizin saldırganlar tarafından bilinmesi gereklidir. Bankacılık, telefon yedekleme, kişisel, sağlık ve benzeri hassas konular için kullandığınız eposta adresiniz ile, diğer işlemler için kullandığınız eposta adreslerini birbirinden ayırın. Size gelen epostanın, beklenen hesabınıza gelip gelmediğini kontrol edin.

7. İki aşamalı kimlik doğrulamaya geçin

İnternet bankacılığında olduğu gibi, kullanıcı adı ve parola girdikten sonra gelen SMS'in web sitesine girilmesi, günümüzde hem Hotmail, Gmail gibi çok kullanılan eposta hizmetlerinde, hem de Linkedin, Facebook, Twitter gibi sosyal medya sitelerinde ücretsiz bir hizmet olarak sunuluyor. Bu özelliği devreye alarak hesaplarınızın koruma kalkanını güçlendirin.

8. "Ödül Kazandınız" ve "Ücretsiz ..." mesajlarına özel dikkat

Bu mesajların neredeyse tümü oltalama saldırılarında kullanılıyor. Yine de emin olmak istiyorsanız ilgili başlığı Internet üzerinde aratarak, gerçek olup olmadığını anlar, daha önce dolandırılan kişilerin bilgilerini görebilirsiniz.

9. Bonus: İmajları kapatın

Teknik bilginiz yeterliyse gelen epostalarda resimlerin (imaj) otomatik yüklenmesini kapatarak güvenliğinizi daha da artırabilirsiniz.

YAZAR HAKKINDA

Murat Lostar yıllar boyunca birçok alanda kazandığı tecrübe sayesinde teknoloji, telekomünikasyon, bankacılık, sigortacılık, tıbbi ürünler, otomotiv, lojistik, makinecilik ve eğlence gibi değişik sektörlerde siber güvenlik hakkındaki bilgi dağarcığını kapsamlı olarak geliştirdi. Murat yaklaşık 30 yıldır bu endüstrinin içinde, bunun 17 yılını özellikle güvenlik üzerine harcadı. Murat sosyal aktiviteler aracılığıyla da bu endüstriye düzenli olarak katkıda bulunuyor. ISACA-Istanbul Chapter kurucu başkanı, (ISC)2 Turkey Chapter kurucu üyesidir. Halen CloudSecurityAlliance-Turkish Chapter'ı yönetiyor. Ayrıca uluslararası etkinliklerde düzenli konuşmacı ve çeşitli üniversitelerde de ders veriyor.