YILDIZ TEKNİK ÜNİVERSİTESİ
BİLGİ İŞLEM DAİRE BAŞKANLIĞI

OLTALAMA SALDIRILARINDAN KORUNMA

YTÜBİDB

OLTALAMA SALDIRILARINDAN KORUNMA

Oltalama saldırısı, günümüzde zararlı yazılımları geçecek denli büyük bir tehdit haline geldi ve iş dünyasına yapılan saldırılarda en başta geliyor. Güvenlik zafiyetlerinin %90'ının sorumlusu olarak oltalama saldırıları görülüyor.

Oltalama saldırılarından korunma için bilinmesi gereken öncelikli ve kolay uygulanabilir ipuçlarını bu yazıda 8 madde ile açıkladık.

1. İyi Bir Açıklama

Oltalama saldırısı; siber suçluların kişisel verileri veya kullanıcı bilgilerini ele geçirmeye çalıştıkları bir saldırı yöntemi. Bunun için özellikle güvenilen markaları veya kullanıcıların tıklaması muhtemel dosya başlıklarını kullanarak zararlı yazılım içeren linkler, web sayfaları, dosyalar, fotoğraflar, dokümanlar kullanıyorlar.

"**Netflix hesabınız donduruldu**" diyen web sayfası linkinden, "**Maaş zamları açıklandı**" diyen word dosyasına varana dek pek çok çeşidine rastlıyoruz.

Bilindik marka logosunu ve web sayfasını birebir kopyalayarak hazırlanmış olan e-posta ve sahte web sayfasında, oltalama konusunda daha önce eğitim almamış kullanıcılar bunun bir saldırı olduğunu anlayamadan bilgilerini çaldırıyor.

Burada önemli bir nokta var; örneğin Office 365 kullanıcı bilgilerini çaldıran kişi Skype, OneDrive, SharePoint gibi bağlantılı hesaplarını da çaldırıyor. Dahası, bu kullanıcı bilgileri olası diğer tüm hesaplarda da deneniyor.

2. Her Şey Taklit Edilebilir

Oltalama saldırılarından korunma için akılda tutulması gereken en önemli noktalardan bir tanesi e-posta adreslerine sadece "görünen"e bakarak güvenmemek gerektiği. Siber suçluların, zararlı yazılım içeren e-postaları gerçek ve güvenilir bir kaynaktan geliyor gibi göstermek için pek çok yöntemi var:

Bu yöntemlerden en sık kullanılanı; e-postaların gönderici isim ve soyadı kısmına microsoftsupport@microsoft.com gibi güvenli bir kaynak adı yazılması ve kurbanların bunun göndericinin e-posta adresi olduğunu zannetmesinin sağlanması.

Aslında gönderici e-posta adresi xxx@yahoo.com iken, kurbanların çoğu gönderici adı yazılı alanı e-posta adresi sanıyor.

Özellikle mobil cihazlarda görüntülenen e-postalarda, gönderici e-posta adresi gizli kaldığı ve çoğu kullanıcı e-posta adresini görüntüle seçeneğini kullanmadığı için saldırganların en sık kullandığı yöntem de bu oluyor.

Bir diğer dikkat edilmesi gereken konu ise tek harf değişikliği yapılan oltalama saldırıları. yildiz@yildiz.edu.tr yerine yildiz@yldiz.edu.tr gibi bir harfi değiştirerek dolandırıcılık yapılmaya çalışılan oltalama saldırılarına da çok sık rastlıyoruz. Benzeri şekilde apple.com yerine apple.co gibi örnekleri de olabiliyor.

Uzantılar ile yapılan sahteciliklere de dikkat etmek gerekiyor. Sadece microsoft.com olması gerekirken microsoft-support.org, microsoft-logins.net, microsoft-securities.com gibi gerçek olmayan alan adları veya aşırı uzun ve karışık alt alan adlarının kullanımı da oltalama saldırılarında karşımıza çıkıyor (icloud.accounts@apple.it.support.zqa.ca gibi)

3. Hızlı Oyna Yanlış Oyna Kuralı

Oltalama saldırısı yapan siber suçluların işi sosyal mühendislik ve bu nedenle insan psikolojisinden anlamak zorundalar. Kurbanlarını panik, aciliyet veya merak duyguları ile fazla düşünmeden hareket etmeye zorlamak için konu başlıklarını buna göre seçiyorlar.

Cazip teklifler: *"Bu e-postayı yanıtlayan ilk 100 kişiye Migros'tan 50TL indirim çeki"*,

Korkutucu haberler: *"Whatsapp hesabınıza erişim sağlandı"*,

Merak uyandırıcı başlıklar: *"2019 yılı ikinci dönem maaş zamları"* gibi konu başlıkları ile gönderilen e-postalar genellikle kullanıcı bilgilerinin çalınması veya finansal zarara uğranması gibi olaylar ile sonuçlanıyor.

Bu e-postaların ortak özelliği kişide hemen hareket etme isteği uyandırması ve bu sayede sahteciliğe dikkat edilememesi. En sık karşılaşılan iki örnek kullanıcının kritik bir hesabının (veya hesaplarının) kapatıldığı veya faturası ödenmediği için bir hesabın askıya alındığı şeklinde.

Kuruluş çalışanlarından birinden geliyormuş gibi görünen ve acil eylem isteyen e-postalar ise çok sık karşılaştığımız BEC (Business E-mail Compromise) olaylarına neden oluyor. CEO'dan finans müdürüne gelen ve belirtilen havale yapılmasını isteyen sahte e-postalar veya bir çalışanın maaş hesabına bağlı banka hesap bilgilerinin değiştiğine dair sahte bilgilendirmeler sonucu kuruluşlar ciddi zararlara uğrayabiliyor.

4. Hedefli Oltalar

Eskiden oltalama saldırıları aynı anda büyük bir gruba gönderilen ve sadece "düşenleri" yakalamaya yönelik saldırılardı. Bu e-postalar jenerik olarak hazırlanıyordu ve kimseyi direkt olarak hedef almıyordu, bu nedenle de sakınması daha kolaydı. Kullanıcıların çoğu kendisine gelen e-postanın adına hitaben yazılması gerektiğini bildiğinden kolaylıkla oltalama e-postalarını ayırt edebiliyordu.

Günümüzde ise oltalama saldırıları kurbanların isimlerinin yer aldığı e-postalar ile kişiye özel olarak yapılıyor hatta konu başlığında kurbanın adı geçiriliyor.

Hatırlarsanız daha da ileriye gidip "porno içerikli görüntüleriniz elimizde" denilen e-postalarda telefon numarası, çoğunlukla eskiden kalma bir parola bilgisi gibi daha kişisel verilere de yer verilmişti.

5. Bu Mesajı Hemen Yanıtlamalısınız

Oltalama saldırılarından korunma için çalışanların kendilerine gelen her e-postayı çok dikkatli okuması gerekiyor. Kimimize günde 150 civarı e-posta geldiğini düşünürsek bu gerçekten çok zor ancak oltalama saldırılarının önemli bir kısmı hedefli oltalama saldırısı haline geldi ve direkt kişiyi hedefleyerek yapıldığı için gerçek bir e-postadan ayırt etmek çok güçleşti. Oltalama saldırılarının çoğu yabancı ülkelerden yapıldığı için en iyi ayırt etme yöntemlerinden biri yazım yanlışları veya düşük cümleleri fark etmek.

6. Bir Link Nelere Kadir

Her oltalama e-postasında kandırmaya yönelik bir bağlantı adresi (link) bulunuyor. Linkte yazılı olan metin "Microsoft hesabınıza gidin" derken, tıkladığınızda yönlendirildiğiniz yer Microsoft'a benzer şekilde hazırlanmış bir sayfa oluyor.

Çalışanlarınızın her bir linke tıklamadan önce fare imleci ile o link üzerine gelerek yönlendirildikleri gerçek sayfayı görüntülemeyi alışkanlık edinmesiyle oltalama saldırılarının büyük bir kısmı engellenebilecektir.

Burada önemli olan ve dikkat edilmesi gereken nokta ana URL'nin doğru olması. Özellikle .com veya .org ile bitmeyen, yine Microsoft örneğinde olduğu gibi gerçek Microsoft.com adresi yerine microsoft-destek.com tarzı adreslere bağlantı veren linklere tıklamamak gerekiyor.

Önemli noktalardan bir başkası; linke tıkladıktan sonra sayfanın sahte olduğunu anlamak yeterli olmayabiliyor. Bağlantıya tıklanması bilgisayara zararlı yazılımın yüklenmesi için yetebiliyor.

Oltalama saldırısı yapan kişilerin yeni favorilerinden bir tanesi de kısaltılmış URL'ler kullanmak. Bu sayede hem e-posta filtrelerini atlatabiliyor hem de kullanıcıları kandırabiliyorlar. Özellikle kısaltılmış URL'lere tıklarken ekstra düşünülmesi gerekiyor.

*Emin olmadığınız bütün linkler için **isitphishing.ai** sayfasını kullanmanızı öneririz.*

7. Eski Fotoğraflarını Buldum, Ekte Gönderiyorum

Her oltalama e-postasında bir link var dedik ancak bu link e-postanın metin kısmında yer almak zorunda değil. Hatta e-posta güvenlik filtrelerini atlatabilmek için e-postanın içerisinde olmaması siber saldırganlar adına daha mantıklı. Metine yerleştirilen oltalama bağlantıları yerine PDF, Word dokümanı vb. gibi ekler ile amaçlarına daha kolay ulaşabiliyorlar. Sandbox gibi teknolojiler e-posta eklerinin zararlı yazılım barındırıp barındırmadığını kontrol ediyor ancak bu eklerin içeriğinde yer alan linklerin ne olduğuna bakmadığı için kolaylıkla temiz görünebiliyorlar. Siber saldırganlar, güvenilir bir iş arkadaşı, firma veya markadan geliyor gibi görünen ve ekte iletilen dokümanı açmanızı isteyen e-postaların içerisinde "güncellemeleri görmek için aşağıdaki linke tıkla" tarzı yazılar ile kurbanlarına rahatça ulaşıyorlar.

8. Sahte mi Gerçek mi?

Markalara ait görsellerin kullanılması, hatta aynı font, aynı tarz, aynı renk olması, logo, isim ve hatta imza barındırması o e-postanın gerçek olduğu anlamına gelmiyor. Tüm bunlar birebir (ve çok kolayca) kopyalanabiliyor. Hatta e-postaların sonlarına bilindik anti-virüs markalarının logo ve yazılarını eklemek (Bu e-posta ... antivirüs ile taranmıştır" gibi) de gördüğümüz kullanıcı kandırmaya yönelik hareketlerden.

Düşüncesizce tıklanan tek bir bağlantının tüm ağı tehdit ettiği düşünüldüğünde, bütün çalışanların aynı dikkat ve özeni göstermesi ve sorumluluk alması, ayrıca dikkatsiz davranışların olası sonuçlarından haberdar olması oluşabilecek zarar verici bir çok olayın önüne geçilebilmesi için elzemdir.

Kaynak: https://sparta.com.tr/ipucu/oltalama-saldirilarindan-korunma-icin-ipuclari/