İletişim

Siber tuzaklar ve oltalama saldırıları

Dijital dünyada güvenli kalmanın yolları

Dijital dünyanın büyümesiyle birlikte, siber saldırılar da giderek daha karmaşık hale geliyor. Oltalama saldırıları, kullanıcıları kandırarak kişisel bilgilerini çalmayı hedefleyen en yaygın yöntemlerden biri. e-Posta dolandırıcılığı, sosyal medya kimlik avı, sahte web siteleri oluşturma ve QR kodları manipüle etme gibi yöntemlerle gerçekleştirilen bu saldırılar, her gün milyonlarca insanı tehdit etse de bunlara karşı çeşitli önlemlerle korunmak mümkün.

Oltalama ya da İngilizcesiyle phishing, bir sosyal mühendislik formu olup saldırganların virüsler, solucanlar, fidye yazılımlar ve reklam yazılımlar gibi zararlı yazılımları yükleyerek ya da kimlik avı teknikleri kullanarak kurbanların parola, kredi kartı gibi hassas bilgilerine yanıltıcı e-posta ya da web siteleriyle ulaşmaya çalıştığı bir dolandırıcılık yöntemi. Oltalama saldırıları, teknolojinin gelişmesiyle birlikte daha karmaşık ve fark edilmesi zor hale geldi. Diğer taraftan teknolojinin gelişmesiyle birlikte oltalama ile mücadele yöntemleri de çeşitlendi ve gelişti. Oltalama, Türk Ceza Kanunu'nun 142/2-e ve 58/1-f maddeleri kapsamında kendisine yer bulan bir siber suçtur. İlk oltalama vakası 1995 yılında AOHell isimli bir bilgisayar programıyla AOL (America Online) isimli dönemin internet servis sağlayıcısı kullanıcılarına yönelik gerçekleştirildi.

Neden Bazı İnsanlar Oltalamaya Daha Eğilimlidir?

İnsanların oltalama mağduru olmasının bazı nedenleri:

1. İnsanlar genellikle başkalarına güvenme eğilimindedir. Oltalama saldırıları, bu güveni kötüye kullanarak, meşru görünen bir kaynaktan (örneğin, bankalar, şirketler veya kamu kurumları) gelen mesajlar gibi davranır. Bu durum, hedefin zararlı içeriğe tıklamayı veya kişisel bilgilerini vermesini kolaylaştırır. İnsanlar doğal olarak güvendikleri kişilere veya kurumlara inanırlar, bu da onları saldırganlar için daha kolay bir hedef haline getirir.

2. Oltalama saldırıları genellikle acil ve önemli bir işlem gerektiriyormuş gibi sunulur. "Fırsatı kaçırmayın!", "Kargonuz iade edilecek.", "Ödemeniz gecikti." gibi ifadeler, kişiyi hemen tepki vermeye zorlar. Bu tür acelecilik duygusu, kişi üzerinde stres yaratır ve daha dikkatli olmasını engeller. Stres altında alınan hızlı kararlar, insanların daha kolay manipüle olmasına neden olabilir.

3. İnsanlar, genellikle bilinmeyenle karşılaştıklarında merak duygusuna kapılırlar. Oltalama saldırıları, "ödül" veya "fırsat" vaatleriyle insanların bu merakını uyandırabilir. Örneğin, "kazandınız" veya "özelleştirilmiş teklifler" gibi mesajlar, insanları bağlantıya tıklamaya yönlendirir.

4. İnsanlar, karmaşık dijital sistemlere

Oltalama Teknikleri Nelerdir?

Bağlantı Manipülasyonu

En sık kullanılan oltalama tekniklerinden biri, sahte bağlantılar oluşturarak güvenilir bir kuruluşu taklit etmektir. Bu yöntemde, web adresleri veya alt alan adları kasten yanlış yazılır ya da gerçek URL'ye en yakın biçimde oluşturularak kullanıcılar yanıltılmaya çalışılır. Örneğin, https://www.cimer.gov.tr/ yerine https://www.cimer.com.tr/ adresi kullanılarak Cumhurbaşkanlığı İletişim Merkezi (CİMER) taklit edilebilir.

Sosyal Mühendislik

Oltalama saldırılarında, kullanıcıları bir bağlantıya tıklamaya, bir eki açmaya veya hassas bilgilerini ifşa etmeye ikna etmek amacıyla sıklıkla sosyal mühendislik teknikleri kullanılır. Dolandırıcılar, genellikle güvenilir bir kaynak gibi davranarak veya bir aciliyet durumu oluşturarak kurbanlarını kandırmaya çalışır. Sosyal mühendislik faaliyetleri, dolandırıcılık yapılacak ülke ve döneme göre değişiklik gösterebilir.

Oltalama Türleri Nelerdir?

E-posta Oltalamaları

E-posta yoluyla gerçekleştirilen oltalama saldırılarında, saldırganlar bireyleri parola veya kart bilgileri gibi hassas verilerini paylaşmaları için kandırmak amacıyla spam e-postalar gönderir. Bu yöntemde saldırılar genellikle toplu olarak yapılır; yani aynı e-posta tek bir kullanıcıya değil, birden çok kullanıcıya ulaşacak şekilde dağıtılır. Saldırganların hedefleri finansal kurumlar, e-posta ve bulut uygulamaları, akış platformları gibi alanlar olabilir. Kullanıcılardan elde edilen bilgiler ya da sağlanan erişim imkânı, genellikle para çalmak, zararlı yazılım yüklemek veya daha spesifik bir oltalama türü olan mızrak oltalama için kullanılır; bu sayede, kullanıcıyla ilişkili diğer bireylerin bilgileri hedeflenir.

Bu tür sosyal mühendislik saldırılarında, gelen e-postalar bankalar, kargo şirketleri veya devlet kurumları gibi güvenilir kaynaklardan geliyormuş gibi görünür ve dili de daha resmî yazılmış olabilir. Bu e-postalarda, kullanıcılar sahte bir internet sitesinin giriş ekranına yönlendirilir ve burada kart şifresi ya da hesap bilgileri gibi hassas verilerini girmeleri istenir.

Mızrak oltalaması

Mızrak oltalaması, toplu oltalama saldırılarından farklı olarak, saldırganların belirli bir hedefe yönelik kişiselleştirilmiş mesajlar ileterek bireyleri kandırmaya çalıştığı bir yöntemdir. Bu saldırılarda, saldırganlar kendilerini devlet kurumu, banka veya kargo şirketi gibi güvenilir bir kuruluş olarak tanıtarak hedef kişiyi yanıltmayı amaçlar. Mesaj içeriğinde, hedef kişiye ait bazı kişisel bilgilere yer verilerek saldırının inandırıcılığı artırılır. Mızrak oltalama saldırıları genellikle üst düzey yöneticiler veya hassas finansal verilere ve hizmetlere erişimi olan finans sektöründeki çalışanları hedef alır.

Sesli Oltalama (Vishing)

Sesli oltalama yönteminde saldırganlar, otomatik ses dönüştürme algoritmalarıyla oluşturulan telefon aramalarıyla çok sayıda kişiyi arayarak, hesaplarında sahte bir işlem tespit edildiğini iddia eder. Arayan telefon numarası, bir banka veya devlet kurumu gibi güvenilir bir kuruluşu taklit edecek şekilde ayarlanır. Bu otomatik çağrılarda, kurbanlardan kart şifresi veya hesap bilgileri gibi hassas verilerini girmeleri istenir ya da kurbanlar sosyal mühendislik teknikleriyle bilgi toplamaya çalışan bir saldırgana bağlanmaya yönlendirilirler.

SMS (Kısa Mesaj Servisi) Oltalaması (Smishing)

SMS oltalaması, SMS veya WhatsApp gibi mesajlaşma uygulamaları üzerinden gönderilen metin mesajlarıyla yapılan bir oltalama saldırısı türüdür. Bu yöntemde, saldırganlar genellikle kurbanları belirli bir bağlantıya, telefon numarasına veya e-posta adresine yönlendirmeye çalışır. Böylece kurbanların hassas bilgilerini ele geçirmeyi hedeflerler. SMS oltalama mesajları, bazen yurtdışı gibi alışılmadık telefon numaralarından gelebilir.

Sayfa Ele Geçirme Oltalaması

Sayfa ele geçirme oltalamasında saldırganlar, kurbanların hassas verilerini toplamak, cihazlarına farkında olmadan zararlı yazılımlar yüklemek veya sahte içeriklerini üst sıralara çıkarmak ve organik trafik elde etmek gibi amaçlarla kötü amaçlı internet siteleri kurar. Bu siteler, genellikle banka veya kamu kurumları gibi güvenilir kuruluşları taklit eder ve kurbanları bu sahte sitelere yönlendirerek hassas bilgilerini ele geçirmeyi amaçlar.

Sosyal Medya Üzerinden Gerçekleştirilen Oltalama Saldırıları

Son yıllarda sosyal medya platformları, oltalama saldırıları için önemli bir hedef haline geldi ve bu platformlar üzerinden gerçekleştirilen saldırılar giderek daha çeşitli ve karmaşık hale geldi. Bu tür saldırılarda saldırganlar, kullanıcıların hassas bilgilerini ele geçirmeyi amaçlar. Sosyal medya hesaplarının giriş sayfalarını taklit ederek kullanıcıların hesap bilgilerini çalabilir, sahte çekilişler ve promosyonlar sunarak kişisel bilgilerini toplayabilir ya da sahte arkadaşlık teklifleri göndererek kullanıcılarla yakınlık kurup zararlı yazılımlar içeren dosyaları indirmelerini veya belirli kişisel bilgilerini (örneğin anne kızlık soyadı) paylaşmalarını sağlayabilirler. Ayrıca sosyal medya platformlarında kullanıcıların hassas bilgilerini ele geçirmek amacıyla sahte anketler, sahte hizmet sunumları ve e-ticaret yönlendirmeleri gibi yöntemler de sıkça kullanılır.

Türkiye Petrolleri Anonim Ortaklığı'nın ana sayfasını taklit eden sahte internet haber sitesi

Ülkemizden Çeşitli Örnekler

Türkiye Petrolleri Anonim Ortaklığı'na yatırım çağrısı:

Kasım 2023'te sosyal medya kullanıcıları, YouTube'da Cumhurbaşkanı Recep Tayyip Erdoğan'ın vatandaşları Türkiye Petrolleri Anonim Ortaklığı şirketine yatırım yapmaya çağırdığı bir video reklamı ile karşılaştı. Reklamı izleyenler, Cumhurbaşkanı Erdoğan'ın şu ifadelerini duydu:

"Ben şahsen Türkiye Petrollerinin yeni yatırım platformunda para kazanamayan herkese 20 milyon lira vereceğim. Artık geleceğiniz için endişelenmenize gerek yok. Finansal refahınız için sorumluluğu üzerimize alıyoruz. Türkiye'de petrol ve doğalgaz arama, üretim ve dağıtım faaliyetlerinde bulunan Türk enerji şirketi olan Türkiye Petrolleri, dikkatini finans ve yatırım sektörüne çevirdi."

Anadolu Ajansı Teyit Hattı, bu durumu inceledi ve videoya reklam veren sayfanın Türkiye Petrolleri Anonim Ortaklığı'nın (TPAO) gerçek internet sitesinin arayüzünü kopyaladığını, ancak alan adının değiştiğini (https://petroleri.com/members.php) ve gerçek TPAO sitesiyle (https://www.tpao.gov.tr/) hiçbir ilgisi bulunmadığını tespit etti.

karşı daha az bilgili olabilir ve bu durum onları manipülasyona daha açık hale getirir. Özellikle teknoloji konusunda bilgisi az olan bireyler, sahte e-postaları ya da sahte web sitelerini doğru bir şekilde ayırt edemezler. Ayrıca, sürekli olarak aldıkları dijital uyarılar ve iletiler, dikkatlerini dağıtarak bu tür saldırılara daha açık hale gelmelerine neden olabilir.

Oltalama ile Bireysel Olarak Nasıl Mücadele Edebiliriz?

- Oltalama saldırıları genellikle hedef kişilerin güvensiz bağlantılara tıklamaları veya kişisel bilgilerini yanlışlıkla paylaşmaları üzerine kurulur. Bu yüzden bireyler, oltalama yöntemlerini tanıyacak şekilde dijital okuryazarlık ve siber güvenlik farkındalık eğitimleri almalıdır.
- Sosyal medya hesapları ve bankacılık uygulamaları gibi hassas bilgiler ve finansal verilerin bulunduğu durumlarda iki faktörlü kimlik doğrulama kullanmak hayatî önem taşır. Böylece oltalama saldırılarında kurbanın bilgileri çalınsa bile o bilgiler kullanılarak ilgili hesaplara giriş istekleri takip edilebilir ve dışarıdan bir kaynak tarafından hassas bilgilere erişim sağlanmak istendiği tespit edilebilir.
- Şüpheli görünen e-posta veya mesajlarda, linklere tıklamadan önce her zaman gönderenin adresini kontrol edin ve e-posta veya mesajdaki bağlantıların gerçek web sitesine yönlendirip yönlendirmediğini inceleyin.
- Bankanızdan geldiğini iddia eden bir mesaj aldıysanız, mesajdaki bağlantıya tıklamak yerine doğrudan bankanızın resmî iletişim kanallarını kullanarak doğrulama yapın.
- Güvenli olmayan e-posta veya telefon aracılığıyla, kişisel bilgilerinizi, banka bilgilerinizi, şifrelerinizi ve diğer hassas verilerinizi asla paylaşmayın.
- e-Posta ve mesajlarda yazım hatalarına dikkat edin. Saldırganlar genellikle taklit ettikleri kişi ya da kurumların isimlerini birkaç harfle değiştirerek sizi yanıltmaya çalışır.
- Güvenmediğiniz e-posta veya mesajlarda bulunan bağlantılara tıklamayın.
- e-Posta veya mesajlarda hassas bilginin talep edilip edilmediğini inceleyin.
- e-Posta veya mesajların geldiği hesabın güvenilir olup olmadığını kontrol edin. Mesaj bir sosyal medya hesabından geldiyse, hesabın onaylı olup olmadığına (örneğin mavi tık olması) dikkat edin ve profilin ne zaman oluşturulduğuna göz atın.
- Eğer mesaj WhatsApp gibi bir mesajlaşma uygulaması ya da SMS ile geldiyse, ilgili numarayı arama motorundan arayarak doğrulamaya çalışabilirsiniz.

19/10/2024 tarihinde Gelir İdaresi Başkanlığı resmî sitesi üzerinden yapılan açıklama

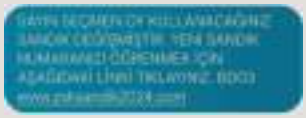
Gelir İdaresi Başkanlığı sitesinin anasayfasını taklit eden sahte internet sitesi

Sahte T.C. Cumhurbaşkanlığı İletişim Başkanlığı Instagram hesabının sponsorla öne çıkarılan hikayesi

Sahte T.C. Cumhurbaşkanlığı İletişim Başkanlığı hesapları

Gerçek Türkiye Cumhuriyeti Cumhurbaşkanlığı İletişim Başkanlığı hesabı

YSK'nın oltalama faaliyetlerine yönelik yazılı açıklaması



31 Mart 2024 Mahallî İdareler Seçimi için gönderilen oltalama SMS'i