Phishing (Oltalama) Saldırısı Nedir?

Phishing, internet tarihinin en eski ve en etkili saldırı türlerinden biridir. Oltalama saldırıları olarak da bilinen bu saldırı türünde genel olarak kurbanların e-posta hesaplarına; hediye, indirim, ödül gibi cezbedici sahte iletiler gönderilir ve kredi kartı bilgileri, kimlik bilgisi gibi hassas verilerin çalınması amaçlanır.

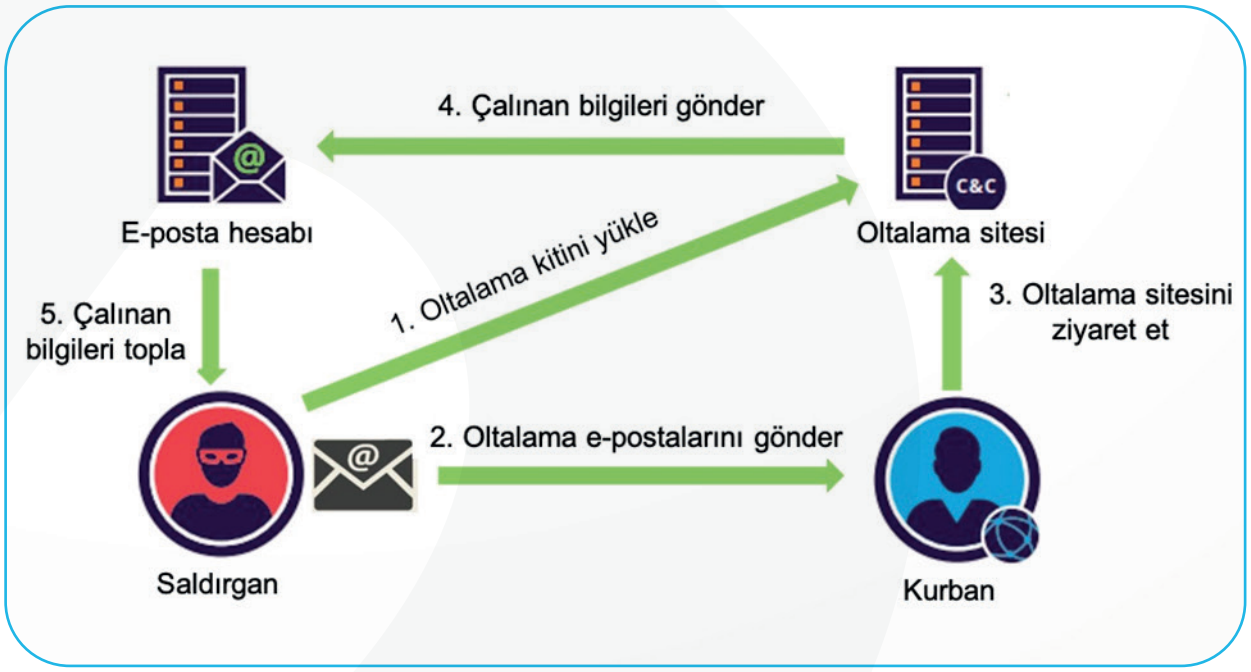
Saldırgan tarafından özel olarak hazırlanan phishing e-postası resmi bir kurumdan geliyormuş gibi ya da gerçek bir e-posta şeklinde görülür. İletilen e-posta mesajlarındaki zararlı bağlantılar tıklandığı zaman kurbanın av olması sağlanabildiği gibi e-postalar ile birlikte ek olarak gönderilen virüslü dosyaların çalıştırılması ile de kurbanların bilgisayarları saldırganlar tarafından ele geçirilebilir.

Phishing saldırılarında kullanılan yem genellikle maaş zammı, hediye, ücretsiz tatil, para ödülü gibi cezbedici senaryolardan oluşturulur.

Kurumlar için büyük riskler oluşturan bu saldırı türüne karşı büyük kayıplar yaşanmaması için çalışanların bilgilendirilmesi ve özel olarak eğitilmesi hayati önem taşır.

Siber saldırganlar phishing yöntemleri ile bilinçsiz kullanıcıları hedefleyerek büyük zararlara sebep olabilir. Phising saldırıları hedefli olarak yapıldığı takdirde ise büyük bir başarı oranına sahiptir.

Doğal olarak siber saldırganlar internet tarihinin en eski ve en etkili yöntemlerinden biri olan phishing saldırılarını sıklıkla kullanmaktadır. Sosyal mühendislik saldırıları ile birlikte gerçekleştirilen spear phishing saldırıları ise maalesef ki siber saldırganların elinde korunması zor ve tehlikeli bir siber silah olarak kurumları tehdit etmektedir.



Oltalama Alan Adları!

Oltalama alan adları, bankalar, e-ticaret siteleri vb. şirketlerin gerçek sitelerinin kopyalarıdır. Kurban giriş bilgilerini (kullanıcı adı ve şifre) veya diğer önemli bilgileri girdiğinde, bu kopya siteden gerçek siteye yönlendirilir.

Oltalama alan adlarından yalnızca çalışanları değil müşterileri de hedef almak için yararlanılır. Şirketler kimlik avı dolandırıcılığından zarar gören müşterilerden doğrudan sorumlu tutulmasalar bile gerekli önlemleri almadığında ciddi itibar kaybı yaşayabilir.

Ad harmanlama (benzer) oltalama alan adları genellikle kolayca karıştırılan harfleri (“u” ve “v” veya “t” ve “f”) değiştirir ve/veya alan adına yeni karakterler ekler. Bu tür teknikler saldırganlar için oldukça etkilidir. Bugün, phishing alan adlarının hedeflerini yakalamak için geçerli SSL ya da TLS sertifikaları vardır. Geçmişte, genellikle ekinde malware içeren phishing e-postalarını görüyorduk. Gelişmiş e-posta filtreleri bu e-postaların geçmesine çoğunlukla izin vermemektedir. Bu nedenle siber saldırganlar tekniklerini malware kullanarak veya e-postalar yerine sosyal medya yayınlarını kullanarak geliştirdiler.

Sosyal Medyada Oltalama

Siber saldırganlar günümüzde oltalama alan adlarının yer aldığı bağlantıyı yaymak için sosyal medyayı oldukça yaygın kullanmaktadırlar. Örneğin Elon Musk’ın adı kullanılarak bir Twitter hesabı üzerinde yapılan oltalama saldırısının bir görseli aşağıda görülebilir.

- Her zaman bir bağlantı içerir (phishing alanına)
- Her zaman bir görsel içerir
- Çoğunlukla kurbanları linke tıklamaları için cazip kılan bir şeyi vadeder.
- Kullanıcılar bu paylaşımları hızlı bir şekilde tespit eder ve yorumlarda uyarılarda bulunur

Oltalama alan adları nasıl bulunur?

Bir şirketin tüm internet ağında arama yapmak ve çalışanlarını ya da müşterilerini hedef alabilecek bir oltalama alan adını tespit etmek çok zordur ancak bazı online ücretsiz araçlar buna yardımcı olabilir. Ayrıca, kimlik avı için kullanılabilecek alan adlarını üreten ve bunların var olup olmadığını kontrol eden Python ile yazılmış bazı yazılımlar da mevcuttur.

Spear Phishing Nedir?

Spear Phishing hedefli oltalama saldırıları olarak tanımlanır. Amaç siber saldırganlar tarafından seçilen kurbanlara ait mahrem bilgilerin, finansal verilerin, banka hesapları gibi benzeri kritik verilerin çalınmasıdır. Rastgele bir kurban seçilebileceği gibi bir kişi veya kurum da hedef alınabilir. Bu durum phishing saldırılarının kurbana göre özelleştirilerek hazırlanmasını gerek-tirmektedir.

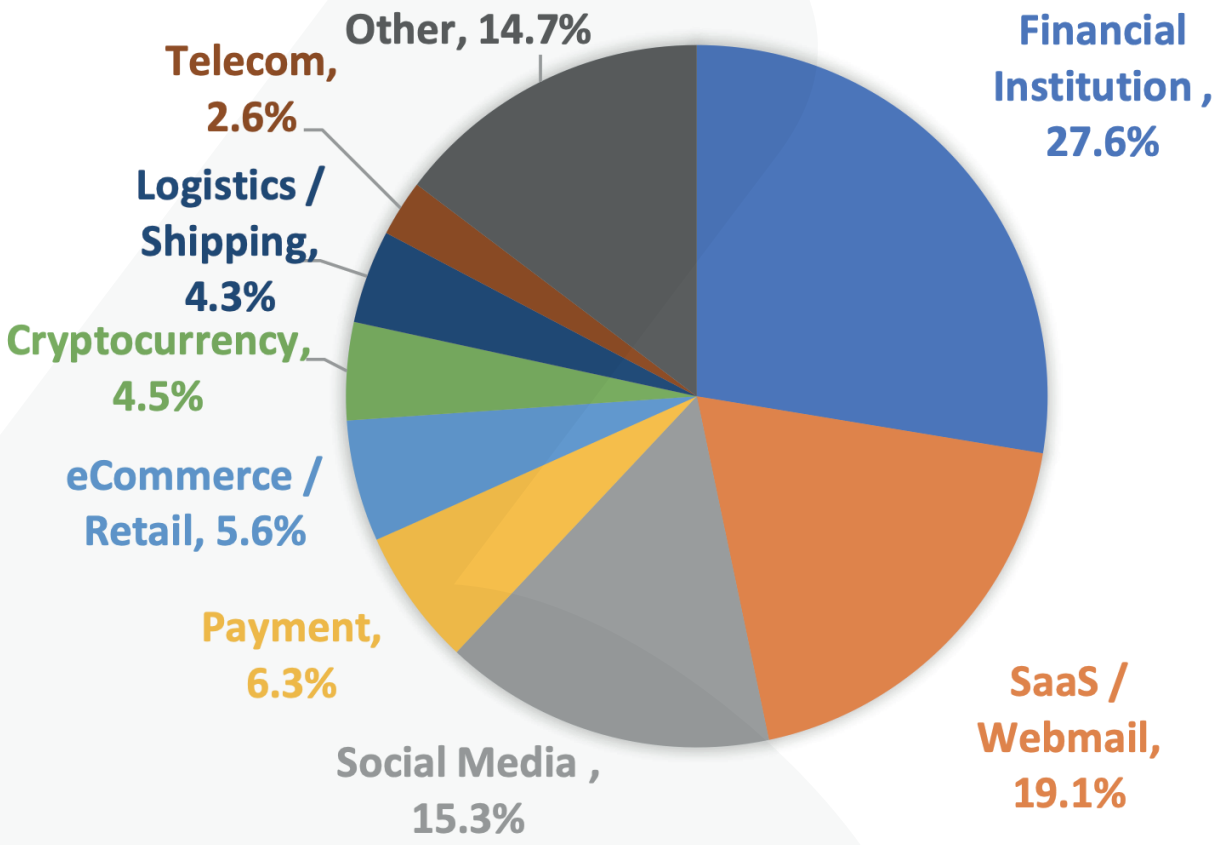
Bu saldırı yöntemi ile bir kuruluşun çalışanlarına ait kimlik bilgileri, sosyal medya hesapları, bankacılık işlemlerinde kullanılan bilgiler elde edilmeye çalışılabilir. Biraz daha ileri boyutta ise ticari sırlar ve gizli bilgiler elde edilebilir. İnternet dünyasında ortaya çıkan phishing saldırılarına baktığımız zaman dünyanın en önemli kurumlarının dahi bu saldırılar karşısında yenik duruma düştüğünü görmekteyiz.

Nasıl gelişiyor?

Spear Phishing saldırılarında ilk ve en önemli adım, kurban olarak seçilen kişi ya da kuruluş hakkında bilgi toplamaktır.

Kurbana iletilen e-posta da kullanılan isimler gerçek kişilere aittir. E-postayı gönderen kişi olarak, yöneticiler, iş arkadaşları veya kurbanın tanıdığı kişiler kullanılır. Aynı zamanda e-postanın içeriğini belirleyebilecek / etkileyebilecek yetkili bir kişi adı ve unvan da seçilir. Bu yöntem sayesinde kurbana, olağan akışta gelebilecek bir e-posta izlenimi verilerek şüphe edilebilecek durumlar ortadan kaldırılır.

APWG Kimlik Avı Etkinliği Trend Raporu'na göre 2022'in 2. çeyreğinde en fazla alan phishing saldırısı alanlar finans kurumları ve Saas/Webmail servisleri olmuştur.



Vishing Nedir?

Vishing, telefonla gerçekleştirilen phishing saldırıları için kullanılan teknik bir kavramdır. Hedef net olarak belirlenerek doğrudan kurbana ulaşılır. Telefon ile yapılan bu saldırı türünde duygusal tetikleyiciler kullanılır. Vishing saldırılarına örnek olarak teknik destek dolandırıcılığı verilebilir. Her iki tür phishing saldırısında da ana amaç kullanıcıdan kritik bilgileri çalmaktır.

Telefon ile gerçekleştirilen Vishing saldırılarında genel olarak; işin acil olduğu, aksi durumda çalışan bir servisin durması, veri kaybı olabileceği gibi ciddi zararlar yaşanabileceği vurgulanarak kurbana korku verilir. Bu sayede karşıdaki kişiye yardım etmek istiyormuş izlenimi verilmiş ve güven sağlanmış olur. Aynı zamanda başarılı bir saldırı için kurbanın merak duygusu da tetiklenebilir.

Oltalama saldırılarından korunmak için ne yapmak gerekir?

Siber güvenlik doğası gereği bütüncül bir güvenlik yönetimine ihtiyaç duymaktadır. Bu noktada oltalama saldırılarına karşı alınabilecek önlemler, diğer saldırı türlerine karşı alınabilecek önlemlerle benzerlik gösterir.

Gelin bu önlemlere birlikte göz atalım;
Fiziksel Güvenlik Önlemleri: Sistem güvenliğinde özellikle de kritik verilerin işlendiği veyahut kullanıldığı şirketlerde fiziksel güvenlik en önemli tedbirlerin başında gelmektedir. Yetkisiz erişimlere karşı fiziksel güvenlik bilgisayar sistemlerinden önce atılan ilk güvenlik adımıdır.

Firewall ve Antivirüs Kullanımı: Hem kurum ağını denetlemek hem de kurum çalışanlarının bilgisayarlarını koruma amacı ile muhakkak bir firewall ve antivirüs kullanılması gereklidir. Birçok kişi firewall varken antivirüs kullanmaya gerek olmadığını düşünse de ikisinin bir arada bulunması gerekir. Bunu şu şekilde düşünebilirsiniz; restoranımızın kapısında duran bodyguard'ı firewall; masaların arasında gezen koruma görevlilerini de antivirüs olarak tanımlayabiliriz. Unutulmamalı ki teknoloji geliştikçe saldırganların teknikleri de gelişiyor. Milyonlarca dolar zarar eden firmalar olduğunu düşünürsek, işletmenizde mutlaka bir firewall cihazı olması gerektiği gibi kullanıcılarınızın bilgisayarlarını korumak için de antivirüs bulundurmak durumundasınız.

Güvenlik Politikalarına Uyum: Kurumların oluşturdukları güvenlik politikaları açık, anlaşılır ve uygulanabilir olmalıdır. Erişilebilirliği eksik veya uygulanabilirliği zor olan güvenlik politikaları çoğu zaman kurum çalışanlarına zorluk yaşatabilmektedir.

Eğitimler ve Yaptırımlar: Kurum çalışanlarının farkındalık düzeyini ölçümlemek ve siber saldırılara karşı bilinçlendirmek için bilgi güvenliği farkındalık eğitimleri verilmektedir. Genel olarak birçok kurum ISO 27001 kapsamında bilgi güvenliği farkındalık eğitimlerini çalışanlarına belirli periyotlarla tekrarlamaktadır. Sosyal mühendislikte en önemli nokta kurum çalışanlarının farkındalık düzeyini artırmakla başlar.

Şüpheci Olmak: Şüpheli durumlar, belirsiz veya ucu açık sorularla veyahut paylaşımlar istendiği takdirde özellikle de e-posta ve SMS erişimlerinde mutlaka şüpheci olmak, gerektiğinde iki kere doğrulamak kurum güvenlik politikalarına yansıtılmalıdır.

Merkezi Loglama: Kurum iç ağı ve kurum çalışanlarının bilgisayarları ile misafir erişimlerinin denetlenmesinin yanı sıra kanunlara uygun bir şekilde log kayıtlarının tutulması gereklidir. Sonuç olarak işletmenizi bu tür saldırılardan korumak için profesyonel bir siber güvenlik hizmeti almak, kaynağından şüphe ettiğiniz e-posta, link ya da reklam bağlantılarına karşı tedbirli olmak ve ekibinizi oltalama saldırılarına karşı bilinçlendirmek hayati önem taşır.

Berqnet Siber Güvenlik Hakkında Detaylı Bilgi:

Logo Teknoloji ve Yatırım Holding A.Ş. çatısı altında faaliyetlerine devam eden Berqnet Siber Güvenlik her ölçekteki işletmenin siber güvenlik ihtiyaçlarına yönelik çözüm üretmek amacıyla 2013 yılında AR-GE çalışmalarına başlayıp 2015 yılında ilk ürün ailesini piyasaya sürmüştür.

Türkiye'de 500'den fazla bayisiyle 7.000'den fazla işletme tarafından tercih edilen Berqnet Siber Güvenlik ürünleri tamamı yerli ve alanında uzman AR-GE kadrosu tarafından işletmelerin veri ve sistem güvenliğinin, yüksek performans ve en doğru çözümlerle korunması için çalışmaktadır. Daha detaylı bilgi almak için 0850 577 23 77 numaralı telefondan bize ulaşabilir ya da www.berqnet.com adresimizi ziyaret ederek tüm ürün, çözüm ve avantajlarımızı yakından tanıyabilirsiniz.

Yararlanılan Kaynaklar:

Berqnet Blog – Firewall ve Antivirüs Kullanımının Önemi - https://berqnet.com/blog/antivirus-nedir
Berqnet Blog – Sosyal Mühendislik Saldırıları Rehberi - https://berqnet.com/blog/sosyal-muhendislik-saldirilari
BGA Bilgi Güvenliği Bilgi Kütüphanesi - https://www.bgasecurity.com/