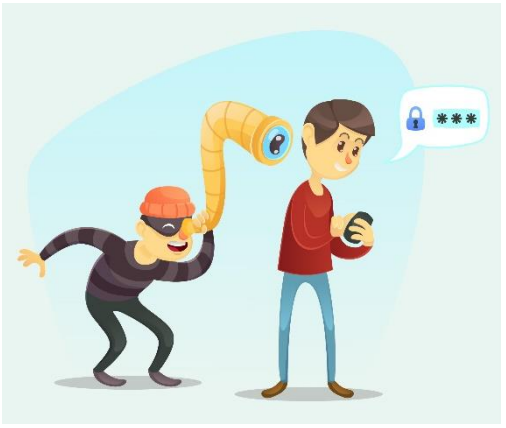
Sosyal Mühendislik

Bu yazımızda insanların en çabuk ve en kolay şekilde hedefleri ele geçirebildiği saldırı çeşitlerinden birisi olan "Sosyal Mühendislik" saldırılarına değinilecektir. Kısaca tanımlamak gerekirse sosyal mühendislik, insanları kandırmayı amaçlayan ve ileri derece teknolojik bilgiye gerek duyulmayan bir saldırı çeşididir. En güçlü güvenlik sistemleri bile çok az teknoloji veya güvenlik bilgisi ile aşılabilmektedir. Sosyal mühendislik birçok şekil, form ve renklerde karşımıza çıkabilir Çoğumuz hayatımız boyunca bir noktada maalesef onun kurbanı olmuşuzdur. Her gün kendine yeni kurban arayan saldırılar günümüzde hem son kullanıcıları hem de işletmeleri etkilemiştir ve etkilemeye de devam etmektedir.

Tarihçesinden bahsedecek olursak, başlangıç zamanı kesin olarak tanımlanamamakta olup tarih boyunca sayısız örneği mevcuttur (Truva Atı) Evrimi ise şu şekilde gerçekleşmiştir:

- Sosyal Mühendislik sadece fiziksel mantıklarla sınırlı kalmayıp, teknolojinin insanların hayatına daha çabuk dokunmasıyla birlikte sahtekarlığı (maalesef) daha kolay bir hale getirdi.
- Saldırganlar oluşturmuş oldukları teknikleriyle daha zeki bir hal aldı.
- E-posta yoluyla çalıştırılabilir (ör: *exe uzantılı dosyalar…) dosya yollamak artık geçmişte kaldı.
- Yazılmış olan zararlı uygulamalar(*.exe) kod karmaşıklaştırma teknikleri ile AV(Anti Virüs)'ler tarafından algılanması zorlaştırıldı ve Powershell'i çalıştırma gibi alternatif yöntemler kullanılmaya başlandı.
- Unicode karakter setinin büyüsüne hâkim olan saldırganlar saldırı çeşitlerini geliştirdiler.

Sosyal Mühendislik Metotları



Genel olarak kabul olan 7 farklı metot vardır. Bunları şu şekilde sıralayabiliriz:

- Can Sıkma
- Oltalama
- Ön Mesaj
- Yakın Takip
- Quid Pro Quo
- Omuz Sörfü
- Çöp Karıştırma

Bu metotlar devam eden bölümlerde örneklerle açıklanacaktır.

1-) Can Sıkma

Hedeflenen kişinin merakına veya aç gözlülüğüne güvenerek, hedefine erişmek için "yem"den ayrılmayı ifade eder. Truva Atı, en büyük mitolojik yem örneklerinden birisidir.
Alternatif örnekler aşağıda listelenmiştir.

- Ücretsiz oyun veya müzik indirilirken formlarda kişisel bilgileri vermeye zorlamak
- İçinde zararlı yazılım olan USB bellekleri ücretsiz olarak dağıtmak.

Maalesef bazı USB'ler cihazlarınıza fazla voltaj verilmesi (USB Killer) nedeniyle donanımınızı da kullanılamaz hale getirmektedir. Bir araştırma sonucuna göre, insanların yaklaşık %76'sı bilmediği donanımları cihazlarına bağlamaktadır. Ofis bilgisayarına bilinmeyen USB bağlanması ise en yaygın saldırı tekniklerden biridir. Yakıcı donanım örnekleri usbkill.com adresinden incelenebilir.

2-) Oltalama

Web sitelerini taklit eden epostalar göndererek yapılan reklamları içerir. Var olan sistemleri taklit ederek kullanıcıları kandırmakla amacıyla kullanılan yöntemdir. Günümüzde görülen en yaygın sosyal mühendislik formlarından biridir. Sahte virüs enfeksiyonu uyarısı (Scareware) yaratmak, Finans kurumlarının giriş sayfalarını birebir kopyalama suretiyle bilgilerin çalınması (özellikle bankalar...), ücretsiz müzik, teklifler vb. yapılan en yaygın saldırı yöntemleri arasında yer almaktadır.

3-) Ön Mesaj

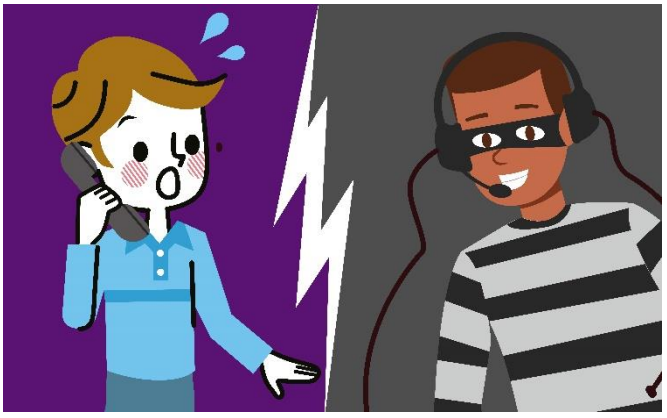
Kurbana, olası olmayan eylemleri gerçekleştirmek için oluşturulan senaryo olarak tanımlanabilir. (Oltalamanın insan karşılığı da diyebiliriz.) Saldırgan güvenilir figürün kimliğine bürünerek saldırı yapmak istediği kişiden bir aksiyon almasını ister. Bu saldırı sahte BT desteği adına yapılan bakım çalışması, yapılan bir araştırma sonucu şirket denetimi ve benzeri senaryolarda iş arkadaşları, polis, vergi makamları ve benzeri roller ile gerçekleşebilir.

4-) Yakın Takip

Saldırganın fiziksel olarak ilgili yere sızmasıdır. Bu saldırı bir senaryo üzerinden örnek ile açıklanabilir. Bir saldırgan kapıyı açık bırakmanızı istiyor, sebebi ise şirket çalışanı giriş kartını (RFID) unutması ve içeri girmek istemesi. Bu saldırı bazı kötü amaçlı yazılımları yüklemek amacıyla basit bir işlem yapma bahanesiyle bir çalışanın telefonunu veya dizüstü bilgisayarını ödünç almakla eşdeğerdir.

5-) Quid Pro Quo

"Bir şey için bir şey" anlamına gelmektedir. Kötü niyetli bir şahıs, BT hizmeti olduğunu iddia eden çeşitli BT şirketlerini arar ve kendini BT departmanından bir çalışan olarak tanıtır. En sonunda saldırgan, sunulan hizmeti gerçekten gerektiren bir çalışan veya şirketle karşılaşacak ve hedefi için saldırısına devam edecektir.



6-) Omuz Sörfü

Kişisel erişim bilgilerini almak için birinin omuzu üstünden bilgisayarına bakma olarak tanımlayabiliriz. Bir bireyin banka hesabı (ATM), telefonunun PIN numarasını veya bilgisayarının parolasını bilinçli olarak izleyerek öğrenme olayı örnek verilebilir. Bu saldırı kameralar sayesinde belirli bir mesafeden yapılabilir.

7-) Çöp Karıştırma

Bir birey, çalışmakta olduğu şirketin verilerini uygun bir şekilde imha etmeden çöpe göndermiş ise çöpü karıştıran bir saldırgan şirketin veya kişinin gizli bilgilerini elde edebilir. Bu metotla banka hesaplarına, kredi kartı numaralarına, sözleşmelere, şirket politikalarına ve benzeri dokümanlara erişilebilir.

Sosyal Mühendislik Nasıl Olur?

Herkese açık olan kaynaklardan bilginin toplanması ile sosyal mühendislik başlar. Bunun için birçok sosyal medya platformundan yararlanılabilir (Google, Facebook, Linkedln, Twitter..). Yardımcı olabilecek yazılımlar veya hazır sistemler de mevcuttur. En popüler sosyal mühendislik sistemleri Maltego, theHarvester ve OSINT Framewor şeklinde sıralanabilir.

Sosyal mühendisliğin bir adımı da bir kişiye ya da kuruma zararlı yazılım yükletmek olabilir. Zararlı yazılımın teslimi için taşıma yöntemi olarak çeşitli formlar kullanılabilir. Kurban olarak seçilen şirket çalışanına gönderilecek telefon, e-posta, web sitesi linki, USB flash bellek gibi medyalar kişinin bu medyayı şirket içerisinde açmasına neden olabilir ve sosyal mühendislik kullanılarak yüklenen yazılım ile sisteme sızmak amaçlanmaktadır. Saldırgan sisteme erişim sağlamak için kurumun bir personeli olduğunu iddia eder ve sistemde yüklü olan kötü amaçlı bir yazılım tespit ettiğini söyler. Bu sayede şüphe uyandırmadan sisteme erişim sağlamayı amaçlar. Saldırgan, saldırıyı planlarken hedef hakkında bildiklerini düşünür. En az şüphe uyandıracak yöntemi belirler. Güçlü ve zayıf yönleri tanımlar ve planı uygulamaya koyar.

Bir Alan Adı Seçin

Burada saldırganın amacı kurumun internet sitesine benzer bir alan adı almak ve çalışanları kandırmaktır. Saldırgan karakter ihmallerini, benzeşen veya tekrarlayan karakterleri kullanarak benzer bir alan adı elde etmeye çalışır, Alan adı değiş tokuşu ya da alan adında değişim yapılabilir mi kontrol eder. Saldırgan bir insanın karıştırabileceği ve farklı algılayabileceği noktaları belirler, Bit flipping (Metin içindeki bir baytı bozarak düz metin içindeki baytı değiştirmek.) metodunu deneyebilir ve Homolyph karakterlerden yararlanabilmektedir. Farklı alan adlarının testinde işe yararlı bir araç olarak URLCrazytool aracından bahsedebiliriz.

Komut ve kontrol merkezi belirleyin

Sosyal mühendislik saldırılarının yönetilmesi için ortak bir sunucu gerekmektedir. Bu gereksinim zorunlu olmamakla birlikte analiz safhasında bilgileri bir araya getirmek konusunda çok daha etkili olacaktır. Merkezi sistemi barındıracak sunucuyu AWS üzerinden kiralamak mümkündür, bu sayede sunucu masrafları daha uygun bir hale gelmektedir. Amazon fiyat konusunda uygun olmakla birlikte çoğu site tarafından güvenilen IP adreslerine sahiptir. Sosyal mühendislik saldırılarını yönetmekte kullanılabilecek ticari ve açık kaynaklı olarak kullanılabilecek birkaç araç aşağıda listelenmiştir.

- Metasploit Framework[1]
- PowerShell Empire Framework
- Çok sayıda çeşitli uzaktan yönetim araçları

FUD ile yük taşıma

Özgür yazılım felsefesini takip eden birçok şifreleme araçları, paketleyiciler ve kod obfuskatörleri bulunmaktadır. Şifreleyici ve RAT'ler çevrimiçi topluluklardan (ör: indetectables.net) elde edilebilir. Bu kaynaklardan elde edilen araçlar antivirüs ve firewall gibi birçok güvenlik çözümüne takılacaktır. Bu çözümlere karşı daha güvenli bir zararlı yazılım elde etmek için küçük değişiklikler yapılması gerekmektedir.

Peki sosyal mühendislik saldırılarına karşı nasıl savunma yapılabilir?

İlk önce şu soruyu kendimize sormalıyız, neden sosyal mühendislik teknikleri bu kadar etkili? Sizce **dikkatsizlik** veya **farkındalık eksikliği olabilir** mi? Kevin Mitnick'in Aldatma Sanatı adlı eserinden birkaç alıntıyı da bu yazıya eklemek istiyorum[2]:
"İnsanlar doğal olarak yardımcı olmak isterler ve bu nedenle kolayca kopyalanırlar."
"Bunun bir çatışmayı önlemek ve bir güven seviyesi olduğunu varsayıyorlar."
"Telefonda güzel sesler duyuyor ve yardımcı olmak istiyoruz."
Bu tür saldırıları aşmak için birtakım çalışmalar yapılabilir. Bunlardan bazıları şu şekilde sıralanabilir:

- Eğitim ve Bilinçlendirme
- Hatırlatma amacıyla yapılan afişler posterler
- Ofislerde TEMİZ MASA politikasının uygulanması.
- En iyi güvenlik uygulamalarını takip edin.
- Kullanmış olduğunuz AV'lerin imza tabanlarını düzenli olarak güncelleyin.
- Bağlantının URL olarak gösterdiğine güvenmeyin.
- Aynı Parolalarınızı 2. defa kullanmayın! Bunun sebebi ise bir saldırgan sizin kimlik bilgilerinizi (parolanızı) alıp çoklu sistemlere erişmek için kullanabilir.

Sorularınız için berkay.dincel@pwc.com adresine mail atabilirsiniz. Herkese güvenli günler diliyorum.

(Dünya, 19.11.2018)

Gökhan Muharremoğlu
Siber Güvenlik Hizmetleri, Kıdemli Müdür
Email: gokhan.muharremoglu@pwc.com

Raif Berkay Dinçel
Siber Güvenlik Hizmetleri
Email: berkay.dincel@pwc.com

Referanslar

[1]-Metasploit Framework - https://www.metasploit.com/
[2]-Kevin Mitnick Aldatma Sanatı- https://www.amazon.com/Aldatma-Sanati-Kevin-D-Mitnick/dp/9757064912