Herkes İçin Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...

Sosyal Mühendislik

Giriş

Siber saldırganların sadece ileri düzey araç ve teknikleri kullanarak kişilerin bilgisayar ve hesaplarına izinsiz olarak girdiği düşüncesi çoğu insanın yaygın bir yanılgısıdır. Bu basitçe doğru değildir. Siber saldırganlar, sizin bilgilerinizi çalmanın, hesaplarınızı ele geçirmenin ya da sisteminize virüs bulaştırmanın en kolay yolunun genellikle sizin yanlış yapmanıza neden olacak şekilde sizi oyuna getirmek olduğunu öğrenmişlerdir. Bu sayıda sosyal mühendislik olarak adlandırılan bu saldırıların nasıl işlediğini ve kendinizi korumak için ne yapmanız gerektiğini öğreneceksiniz.

Konuk Yazar

James Lyne (**@jameslyne**), sertifikalı SANS eğitmeni ve Sophos'da küresel araştırma başkanıdır. Siber suçluların en güncel ve en büyük yaratımlarını çözer ve geri mühendislik yapar. Ayrıca SANS'da Metasploit (SEC580) ve Sosyal Mühendislik (SEC567) derslerinin yazarıdır.

Sosyal Mühendislik

Sosyal Mühendislik, saldırganın sizin yapmamanız gereken bir şeyi yapmanıza neden olacak şekilde sizi oyuna getirdiği psikolojik bir saldırıdır. Sosyal mühendislik kavramı yeni değildir, binlerce yıldır varolmuştur. Dolandırıcıları ya da sahtekarları düşünün, bunun ta kendisidir. Siber saldırganlar için bugünün teknolojilerinin bu kadar çok verimli olmasının sebebi onları fiziksel olarak görememeniz, onların istedikleri herşey ve herkes gibi olabilmesi ve siz dahil dünya çapında milyonlarca insanı hedef alabilmeleridir. Ayrıca sosyal mühendislik saldırıları bir çok güvenlik teknolojisini atlatabilmektedir. Bu saldırıların nasıl işlediğini be kendinizi bunlardan nasıl korumanız gerektiğini anlamanın en kolay yolu iki gerçek hayat örneklerine bakmaktır.

Size bilgisayar destek şirketinden, internet hizmet sağlayıcınızdan ya da belki Microsoft teknik desteğinden, olduğunu söyleyen bir kişiden bir telefon gelir. Arayan kişi bilgisayarınızın aktif olarak interneti taradığını, bilgisayarınıza virüs bulaşmış olduğuna inandıklarını ve bilgisayarınızı korumada size yardım etmek için görevlendirildiklerini açıklarlar. Daha sonra birçok teknik terim kullanır ve bir çok kafa karıştırıcı adımla sizi bilgisayarınıza virüs bulaştığına ikna etmeye çalışır. Örneğin, sizden bilgisayarınızda bazı dosyaların olup olmadığını kontrol etmenizi isteyebilirler ve bu dosyaları bulma konusunda size yol gösterebilirler. Bu dosyaları bulduğunuzda arayan kişi bu dosyaların sizin bilgisayarınıza virüs bulaştığını kanıtladığına sizi inandırır ama gerçekte bu dosyalar dünyadaki hemen hemen her bilgisayarda bulunan yaygın sistem dosyalarıdır. Sizi bilgisayarınıza virüs bulaştığına ikna ettiklerinde, sizi onların güvenlik yazılımlarını almaya ya da problemi çözebilmek için uzaktan erişim bilgilerinizi onlara vermeye zorlarlar. Ancak sattıkları yazılım, gerçekte kötü niyetli bir programdır. Eğer alır ve bilgisayarınıza kurarsanız sadece kendi bilgisayarınıza virüs bulaştırmak için kandırılmış olmazsınız, bunun için onlara para ödemiş olursunuz. Bilgisayarınıza uzaktan erişim için bilgilerinizi

Sosyal Mühendislik

verirseniz, bilgisayarınızı ele geçirirler ve verilerinizi çalar ya da açık arttırmada satılmak üzere kullanırlar.

Bir diğer örnek ise CEO Dolandırıcılığı olarak adlandırılan ve daha çok iş yerinde görülen e-posta saldırılarıdır. Bu, siber saldırganın şirketinize çevrim-içi olarak eriştiğinde ve patronunuzun ve birlikte çalıştığınız kişilerin isimlerini tespit ettiğinde gerçekleşir. Saldırgan daha sonra sanki o kişi imiş ve bu e-posta o kişiden geliyormuş gibi yaparak sizin için bir e-posta hazırlar. Bu e-posta acil olarak sizden banka havalesi yapmak ya da çalışanların hassas bilgilerini göndermek gibi bir konuda harekete geçmenizi ister. Çoğunlukla bu e-postalar sizin güvenlik prosedürlerini atlamanızı gerektirecek şekilde acilmiş gibidirler, örneğin sizden çok hassas bilgileri kişisel bir @gmail.com uzantılı e-posta adresine göndermenizi isteyebilirler. Bunun gibi hedeflenen saldırıları çok tehlikeli yapan şey siber saldırganların araştırmalarını daha önceden yapmış olmalarıdır. Bununla birlikte, antivirüs ya da güvenlik duvarı gibi güvenlik teknolojileri, ortada kötü niyetli bir yazılım ya da bağlantı olmadığından dolayı bu tip saldırıları tespit edemez ve engelleyemez.

Sağduyunuz, sosyal mühendislik saldırılarını tespit etmekte ve durdurmakta sizin en güçlü savunmanızdır.

Buna benzer sosyal mühendislik saldırılarının sadece telefon aramaları ya da e-postalar ile sınırlı olmadığını aklınızda bulundurun. Telefonunuza gönderilen, sosyal medyadan iletilen ya da şahsen verilen metin mesajları dahil herhangi bir formda karşınıza çıkabilir. Buradaki önemli nokta neye dikkat edeceğinizdir, siz kendinizin en iyi savunucususunuz.

Sosyal Mühendislik Saldırılarının Tespit Etmek ve Durdurmak

Neyse ki bu tür saldırıları durdurmak düşündüğünüzden daha kolaydır – sağduyunuz sizin en iyi savunmanızdır. Eğer herhangi bir şey şüpheli görünüyorsa ya da iyi hissettirmiyorsa, bu bir saldırı olabilir. Bir sosyal mühendislik saldırısının en yaygın ipuçları aşağıda verilmektedir:

- Biri çok fazla derecede aciliyet oluşturuyorsa, sizin yanlış yapmanıza neden olacak şekilde sizi kandırmaya çalışıyordur.
- Biri sizin hesap numaranız gibi erişmemeleri gereken ya da daha önceden bilmiş olmaları gereken bir bilgiyi sizden istiyorsa
- Biri sizden şifrenizi istiyorsa ki hiçbir yasal şirket bunu sizden istemez.
- Biri iş yerinde takip etmeniz gereken güvenlik prosedürlerini atlamanız ya da görmezden gelmeniz konusunda zorluyorsa
- Herhangi bir şey inanılmayacak kadar iyi görünüyorsa. Örneğin çekilişe katılmamış olmanıza rağmen piyangoyu ya da bir iPad'i kazandığınız size bildirilmişse.

Sosyal Mühendislik

- Arkadaşınızdan ya da iş yerinde beraber çalıştığınız kişiden gerçekten onlardan geldiğini hissetmeyen bir üslupla yazılmış olan garip bir e-posta geldiyse. Siber saldırgan onların hesabını ele geçirmiş ve sizi kandırmaya çalışıyor olabilir. Kendinizi korumak için bu tür istekleri arkadaşınıza yüz yüze ya da telefon gibi farklı bir iletişim yöntemi kullanıp ulaşarak doğrulayın.

Eğer birinin sizi oyuna getirdiği konusunda şüpheleniyorsanız, o kişi ile bir daha iletişim kurmayın. Eğer saldırı iş ile ilgili ise, yardım masasına ya da bilgi güvenliği ekibine hemen bu durumu bildirdiğinizden emin olun. Unutmayın, sağduyu çoğunlukla sizin en iyi savunmanızdır.

Daha Fazla Bilgi İçin

Aylık OUCH! güvenlik farkındalığı bültenine üye olun, OUCH! arşivlerine erişin ve securingthehuman.sans.org/ouch/archives adresini ziyaret ederek SANS güvenlik farkındalığı çözümleri hakkında daha fazla bilgi edinin.

Türkçe Çevirisi

Selma Süloğlu, ODTÜ Bilgisayar Mühendisliğinde doktorasını tamamlamış olup SOSoft Bilişim Teknolojilerinde biyometrik güvenlik sistemleri üzerinde çalışmaktadır.

Sema Yüce, Türkiye'nin önde gelen kurumsal şirketlerinde ve özellikle bilişim, telekomünikasyon, sanayi, perakendecilik gibi sektörlerde; bilgi güvenliği, iş sürekliliği, risk yönetimi, altyapı hizmetleri, yazılım geliştirme ve proje yönetimi alanlarında yönetici ve danışman olarak 15 yılı aşkın süredir görev yapmaktadır.

Kaynaklar

Oltalama:	https://securingthehuman.sans.org/ouch/2015#december2015
CEO Dolandırıcılığı:	https://securingthehuman.sans.org/ouch/2016#july2016
Fidye Yazılımlar:	https://securingthehuman.sans.org/ouch/2016#august2016
OUCH Arşivleri:	https://securingthehuman.sans.org/ouch/archives

Yayın Kurulu : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley