Bilgisayar Kullanıcıları için Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...

Evet, Siz Gerçekten Hedefsiniz

Giriş

Birçok insan siber suçluların hedefi olmadığını düşünerek genel bir yanılgıya düşmektedir, kendilerinin ya da bilgisayarlarının bir değer taşımadığını düşünürler. Oysa ki bu düşünce gerçeklerden çok uzaktır. Eğer bir bilgisayarınız, mobil cihazınız, çevrim-içi hesabınız, e-posta adresiniz, kredi kartınız varsa ya da çevrim-içi bir etkinliğe katılmışsanız siber suçlular için uğraşmaya değersiniz. Bu bültende neden bir hedef olduğunuzu, nasıl saldırılara uğrayabileceğinizi ve kendinizi korumanız için neler yapabileceğinizi açıklayacağız.

Konuk Editör

Backshore Communications'ın başkanı ve CTO'su olan Eric Conrad, CISSP Study Guide, İkinci basım ve Eleventh Hour CISSP, 2. basım kitaplarının başyazarıdır. Ayrıca SANS'da altı günlük Continuous Monitoring and Security Operations (SEC511) kursunun da ortak yazarıdır.

Neden Siz Hedefsiniz?

Dolandırıcılık, kimlik hırsızlığı ve gasp gibi suçlar medeniyetlerin kurulmasından beri var olan hayatımızın ayrılmaz bir parçasıdır. Bir suçlunun hedefi her zaman aynıdır: en az riskle kolayca, kazanabildiği kadar para kazanmak. Eskiden suçlular bulundukları mekan ile sınırlı olduklarından ve kurbanlarının yanında fiziksel olarak bulunmaları gerektiğinden bu zor bir işti. Sadece hedef alabilecekleri kişiler onları sınırlamıyordu, ayrıca büyük bir riski de göze almaları gerekiyordu. Ancak suç, internet ve çevrim-içi teknolojilerinin gelişi ve kullanılmasıyla köklü bir şekilde değişti. Şu an siber suçlular neredeyse dünyadaki herkesi az maliyetle ya da hiç masrafsız bir şekilde ve çok az riskle kolayca hedef alabiliyorlar. Ayrıca siber suçlular eskisinden daha etkili, oldukça organize ve etkili bir hale geldiler.

Sonuçta siber suçlular ne kadar çok kredi kartı çalarlarsa, ne kadar çok banka hesabı ele geçirirlerse ya da ne kadar çok şifre çalarlarsa o kadar çok para kazanacaklarını biliyorlar. Siz dahil internete bağlı herkesin bilgilerini ele geçirmeye çalışacaklardır. Tüm dünyadaki insanların bilgilerin ele geçirmek çok büyük bir iş gibi görünse de onların yerine iş yapan otomatik araçlar kullandıklarından bu iş şaşırtıcı bir şekilde kolaydır. Örneğin, milyonlarca e-posta adresinin olduğu bir veri tabanı kurarak otomatik araçlar yardımıyla oltalama mesajlarını tüm bu e-posta adreslerine gönderebilirler. Bu mailleri göndermenin siber suçlara bir maliyeti yoktur: pis işlerini yapmak için basitçe ele geçirdikleri bilgisayarları kullanırlar, bu sizinki bile olabilir. Bu sizin bilgisayarlarınızın ne derece değer taşıdığını gösteren başka bir örnektir ve hiç bir şey olmasa bile diğer insanların bilgilerini ele geçirebilmek ya da zarar vermek için kullanabilirler. Sonuç olarak, bu suçlular e-posta saldırılarında kimlerin ağlarına düşeceğini bilemezler ama ne kadar çok kişiye e-posta gönderirlerse o kadar çok kişinin kurban olabileceğini bilirler. Ya

Evet, Siz Gerçekten Hedefsiniz

da belki de bu suçlular internetteki bütün bilgisayarları tarayarak (bunu yaparken ele geçirilmiş bilgisayarlarını kullanırlar), ele geçirebilecekleri bilgisayarları ya da cihazları bulmaya çalışırlar. Unutmayın, sizin seçilmemiş olmanız, özel olduğunuz anlamına gelmez. Bu suçlular olabilecek herkesi hedef seçerler, siz dahil.

Fark etmeyebilirsiniz ama cihazlarınız ve bilgileriniz dünya çapında siber suçlular için çok büyük değer taşır.

Kendinizi Koruma

Siber suçlular dünyadaki kişilerin bilgilerini ele geçirmeye çalışırken nispeten basit metotlar kullanırlar. Neyse ki siz de basit adımları takip ederek kendinizi koruyabilirsiniz. Tavsiye ettiğimiz bazı adımlar aşağıda açıklanmaktadır:

- **Kendiniz**: En nihayetinde siz siber saldırılara karşı ilk savunma hattını oluşturursunuz. Birçok saldırı, bir siber suçlunun bulaşmış e-posta eklerini açmanızı sağlayacak şekilde oyuna getirmesi ya da telefonla şifrenizi sizden almak için sizi kandırması gibi olaylarla başlar. Sağduyunuz sizin en iyi savunmanızdır. Eğer herhangibir şey saçma, şüpheli ya da inanılmayacak kadar iyi görünüyorsa bu büyük ihtimalle bir saldırıdır.

- **Güncelleme**: Bilgisayar ya da mobil cihazınızın tam olarak güncellendiğinden ve en güncel yamaların yüklendiğinden emin olun. Bu sadece sizin işletim sisteminiz için önemli değildir, aynı zamanda bu uygulamalarınız ve eklentileriniz için de büyük önem taşır. Sisteminizi ve uygulamalarınızı sürekli güncel tutarak en yaygın saldırılara karşı kendinizi koruyabilirsiniz.

- **Şifreler**: Her hesabınız için güçlü ve eşsiz şifreler kullanın. Bu yolla kullandığınız bir ağ sitesi tüm şifreler ile birlikte ele geçirildiğinde, sizinkisi dahil, diğer hesaplarınız güvende olacaktır. Ayrıca, farklı cihazlarınızın güçlü ve eşsiz bir şifre, PIN ya da diğer kitleme yöntemleriyle korunmasını sağlayın. Tüm şifrelerinizin kaydını tutmak için şifre yöneticisini kullanmanızı öneriyoruz.

- **Kredi Kartları**: Mali çizelgenizi en azından haftada bir kontrol edin, çünkü aylık kontrol yeterli değildir. Sizin izniniz haricinde kredi kartınız ile yapılan bir harcama gördüğünüz anda hemen bankanızı arayarak onları durumdan haberdar edin. Eğer bankanız normalden uzun ve garip işlemler olduğunda size e-posta ya da mesaj alarmları gönderme seçeneği sunuyorsa şüpheli bir faaliyette hızlı bir şekilde bildirim almak için sunulan bu özelliği kullanın.

Evet, Siz Gerçekten Hedefsiniz

- **Ev Ağınız**: Ev ağınız için kullandığınız WiFi ulaşım noktalarını güçlü bir yönetici şifresi ile koruyun. Wi-Fi ağınıza dahil olmak isteyen herhangibir kişinin bu şifre ile giriş yapmasını sağlayın. Ayrıca, hangi cihazların ev ağınıza bağlı olduğunu bilin ve bu cihazların hepsinin güncel olduğundan emin olun.

- **Sosyal Medya**: Kendiniz ile ilgili ne kadar çok bilgiyi çevrim-içi gönderirseniz o kadar kendinizi riske atarsınız. Bu bilgiler sadece siber suçluların sizi hedef seçmeleri için kolaylıkla kullanabilecekleri, kandırabiliecekleri bilgiler değildir, aynı zamanda her bilgi sizi gerçekten tanımlayarak sizi daha değerli bir hedef yapar.

Daha Fazla Bilgi İçin

Aylık OUCH! güvenlik farkındalığı bültenine üye olun, OUCH! arşivlerine erişin ve http://www.securingthehuman.org 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

OUCH! Şifre Yöneticileri:	http://www.securingthehuman.org/ouch/2013#october2013
OUCH! Ev Ağınızı Koruma:	http://www.securingthehuman.org/ouch/2014#january2014
OUCH! Oltalama Saldırıları:	http://www.securingthehuman.org/ouch/2013#february2013
Poster: Siz Hedefsiniz:	http://www.securingthehuman.org/resources/posters

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