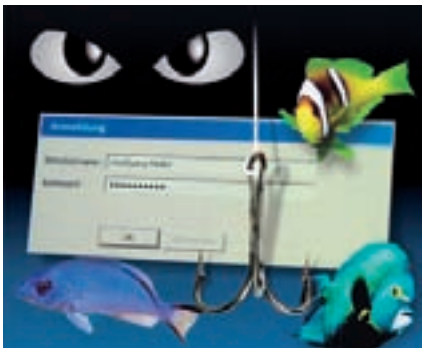
DİKKAT! KİMLİĞİNİZ ÇALINDI!

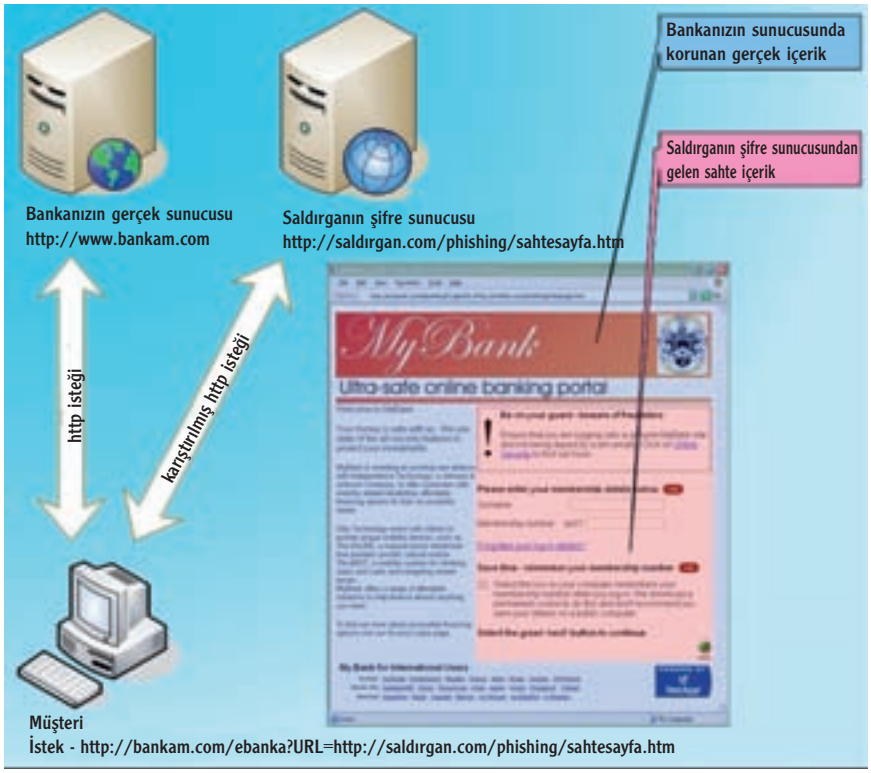
İnternet üzerinde yer alan sanal alışveriş sitelerinin kullanım oranındaki artışla ve geniş bant aralığındaki İnternet bağlantıların yaygınlaşmasıyla birlikte, masum kullanıcıları hedef alan bilgisayar korsanlarının amaçlarına ulaşmak için kullanabilecekleri olanaklar da arttı. Yapılan araştırma sonuçları, 2005 yılında sanal kimlik hırsızlarının yalnızca ABD'deki kurbanlarına maliyetinin yaklaşık 265 milyon dolar olduğunu gösteriyor. Resmi verilere göreyse 2004 yılındaki dolandırıldığını belirten tüketicilerin %53'ünün şikayeti İnternet tabanlı işlemlerle ilgili. Yetkililer, sanal alemde suç işlemenin, uyuşturucu kaçakçılığından daha kârlı bir endüstri haline geldiği iddiasında. Tehlike bu kadar büyük olunca, biz İnternet kullanıcılarına da tedbiri elden bırakmamak düşüyor.

Kalabalık bir caddede ya da alışveriş merkezinde gezerken cüzdanımızı çantamızın kolayca ulaşılabilecek bir bölümüne koymanın gerçek dünyada başımıza gelebilecek bir yankesicilik olasılığını artırdığı açık. Aynı şekilde son yıllarda yaşanan teknolojik gelişmeler sayesinde artık bankacılık işlemlerimizi ve alışverişlerimizi İnternet üzerinde yapabiliyor olmamız da, sanal dünyada uğrayabileceğimiz yankesicilik ve dolandırıcılık olaylarına karşı savunmasızlığımızı artırıyor. İnternet kullanımının yaygınlığı konusundaki araştırma sonuçları bu savunmasızlığımızın kökenlerini net biçimde açıklıyor: Geniş bant aralığıyla İnternet'e sürekli bağlı kişilerin oranı 2004 yılının Ağustos ayında %51,4 iken, 2005 yılının Ağustos ayında %61,3'e çıkmış. İnternet bankacılığını kullanan kişilerin sayısı 2002-2004 yılları arasında %47 artış göstermiş. İnternet üzerinden yapılan sanal alışverişlerin büyüklüğüyse 2004 yılında bir önceki yıla göre %26'lık bir artış göstererek 65 milyar dolarla tepe noktasına ulaşmış. İnteernet'e bağımlılığımız ve parayla ilgili her türlü işlemlerimizi İnternet üzerinden gerçekleştirme oranımız bu hızla arttıkça, savunmasızlığımızın artması da kuşkusuz kaçılmaz oluyor. Geçtiğimiz yıl sanal alemde boy gösteren kimlik hırsızlarının yalnızca Amerika'daki kurbanlarının sayısının yaklaşık 10 milyon kişi olması da, bunun temel bir göstergesi.



"Mış" Gibi Davranmak

Aslında birilerinin kimlik bilgilerini ele geçirerek o kişiymiş gibi davranmak, tarihin çok eski dönemlerinden beri varolan bir suç türü. Ancak günümüzün teknolojik gelişmeleri sayesinde bu suç türü altın çağını yaşıyor. Bu tür dolandırıcılıkların en zararlılarından biri "phishing" yöntemi. İsmini İngilizce'de eskiden telefon sistemlerinden ücretsiz görüşme yapmak için kullanılan bir aldatmaca sistemi anlamına gelen "phreaking" ve balık avlama anlamına gelen "fishing" sözcüklerinin birleşmesinden alan bu yöntemin te-



melinde biz masum İnternet kullanıcılarını sahte e-postalar yoluyla kandırmak yatıyor. Dolandırıcılar önce kurbanlarının hangi bankayla çalıştığını ya da hangi sanal alışveriş sitesini kullandıklarını öğreniyorlar. Ardından da bu bankadan ya da alışveriş sitesinden gönderilmiş gibi görünen bir e-postayı kurbanlarına gönderiyorlar. Bu e-postada yer alan bir bağlantıya tıklayarak sözü geçen İnternet tabanlı uygulamalara giriş yapmak için kullandıkları kişisel bilgilerini güncellemeleri gerektiği, aksi takdirde güvenlikle ilgili sorun yaşayabilecekleri yazıyor. Gönderilen e-posta, birebir ilgili kurumdan gönderilmiş izlenimi verecek şekilde tasarlandığından çoğu kişi bunun sahte bir bildirim olduğunun farkına varmıyor ve e-postada yer alan bağlantıya tıklayarak gerekli güncellemeleri yapıyor. Bunu yapmasıyla birlikte de, kendisine özel tüm kişisel ve finansal bilgileri dolandırıcıların ellerine teslim etmiş oluyor. Çünkü e-postada yer alan bağlantıya tıklayarak girdiği ve bu bilgi güncellemelerini yaptığı web sitesi, aslında dolandırıcıların kurbanlarının kullandığı İnternet bankacılığının ya da sanal mağazanın sitesine birebir benzeyecek şekilde tasarladıkları sahte bir site.

"Ben çok iyi bir bilgisayar kullanıcısıyım ve bu tür basit numaraları asla yutmam!" diyorsanız, bir kez daha düşünmenizi öneririz. Çünkü bir pazar araştırma şirketi olan Gartner'ın verilerine göre 2004 yılının Mayıs ayıyla 2005 yılının Mayıs ayları arasındaki 12 aylık bir dönemin sonunda yaklaşık 2,4 milyon Amerika'lı yetişkin "phishing" yöntemiyle yapılan dolandırıcılıkların kurbanı olmuş. Bu saldırıların bankalara, tüketicilere ve tüccarlara toplam maliyetiyse 929 milyon dolar. Bir yandan İnternet kullanıcılarının bilinç düzeyi artıyor olsa da bu tür saldırıların sayısı da hızla çoğalmakta. Geçen yıl bu yöntemi kullanarak dolandırıcılık yapanlar tarafından hedef alınan bankaların ve e-ticaret sitelerinin sayısının iki katından daha fazla artmış olması da bunun açık bir göstergesi.

Üstelik kullanıcılar herhangi bir tür yönteme karşı uyanıklık düzeylerini artırdıkça, dolandırıcılar da boş durmayıp yeni yöntemler geliştiriyorlar. "Pharming" olarak bilinen bir yöntem, bankalara ve alışveriş sitelerine ait yasal siteleri barındıran sunucuların korsanlar tarafından ele geçirilmesi ve daha sonra bu sitelerin müşterilerinin birebir yasal örneklerine benzeyen sahte sitelere yönlendirilmesi anlamına geliyor. Bu dolandırıcılık türü "phishing" yönteminden daha tehlikeli. Çünkü size gönderilen e-postada yer alan bağlantıya tıklamanızı ve açılan site üzerinden kullanıcı bilgilerinizi değiştirmenizi gerektiren "phishing" yönteminde olup bitenler, en azından belli bir aşamaya kadar, sizin kontrolünüzde gerçekleşiyor. Ancak "pharming" denen dolandırıcılık türünde her şey bütünüyle sizin kontrolünüz dışında oluveriyor. Dolandırıcılar tarafından gizlice bilgisayarınıza bırakılan ve bilgisayarınızın belli bir bölümünde sürekli saklanan bir değişken, Truva Atı olarak adlandırılan bir yazılım parçası kullanıyor. Bu yazılım parçası, Web tarayıcınızda geçmişte girdiğiniz sitelere ait bilgilerin saklandığı kaşenizle oynuyor ve o sırada ziyaret ettiğiniz sitenin yeniden yükleniyormuş gibi görünmesini sağlıyor. Böylece herhangi bir İnternet bankacılığı ya da e-ticaret sitesini ziyaret etmeye çalışırken hiç haberiniz olmadan dolandırıcıların hazırlamış oldukları sahte sitelere yönlendiriliyorsunuz ve bu siteler üzerinden size ait tüm bilgiler hırsızların eline ulaşıyor.

Kablosuz Bağlantılardan Zombi Bilgisayarlara

Günümüzde iyice yaygınlaşmış olan kablosuz İnternet bağlantı noktalarıysa, sanal kimlik hırsızları için yeni bir uygulama ortamı. Saldırganlar önce pek çok kafede ya da lokantada bulunan kamuya açık kablosuz ağlar üzerine yerleşiyorlar. Ardından bu ağın üstüne bindirmek amacıyla yakınlarda

kendilerine ait bir kablosuz İnternet bağlantı noktası kuruyorlar. Saldırganların kurduğu bu bağlantı noktalarına "kötü ikizi" anlamına gelen "evil twin" bağlantı deniyor. Bu aşamadan sonra sıra kurbanların bu ağa bağlanmaları için beklemeye geliyor. Kurbanlar sahte İnternet ağını kullanırken, bu ağı kuran suçlular da kurbanların hareketlerini izliyorlar ve bu kişilere ait tüm bilgileri ele geçiriyorlar.

Sanal alemdeki dolandırıcılıklar içinde en ürpertici olanlarından biriyse, evinizde kullandığınız kişisel bilgisayarınızın hiç tanımadığınız bir yabancıya karşı yapılacak bir saldırıda görevlendirilmek amacıyla seçilmiş olabileceği. Çoğu sahte web sitesi, sanal dolandırıcıların korsanlıkla ele geçirdikleri ev bilgisayarlarına kurulmuş Web sunucularında barındırılıyor. Bu şekilde ele geçirilen bilgisayarlara zombi bilgisayar adı veriliyor. Bu zombi bilgisayarlara dışarıdaki bir kişi tarafından kontrol edilmeye olanak veren uzaktan erişilir bir Truva Atı yazılım parçası bulaştırılmış oluyor. Bu makinelerden binlercesine aynı anda ulaşabilen sanal dolandırıcılar, bu bilgisayarları sahte e-postalar göndermek ya da sahte Web sitelerini barındırmak için kullanıyorlar. Kısaca "bot ağlar" olarak adlandırılan bu robot ağları suçlulara bir yandan bir çok makineyi aynı anda kontrol edebilme olanağını verirken, bir yandan da kendilerini bütünüyle bir isimsizlik katmanı altında gizlemelerini sağlıyor.

Üstelik bu yöntemde suçluların girişimlerini kazançlı bir iş haline getirmeleri için yığınlarca kurbana gereksinimleri yok. Çoğu zaman birkaç kurban bile onlar için yeterli olabiliyor. Bu duruma en iyi örneklerden biri Ekim ayında her ikisi de Las Vegas'ta yaşayan 28 yaşındaki Westley Kostelec'in ve 29 yaşındaki Ted Stewart'ın durumu. Sahte e-postalar göndermek ve U.S Bank'ın görünümündeki sahte siteleri barındırmak amacıyla ev bilgisayarlarını ele geçirmeleri nedeniyle bilgisayar dolandırıcılığından suçlu bulunan bu iki siber soyguncu, yalnızca 10 kurbanı ağlarına düşürerek kabaca 300.000 e-posta göndermişler ve bu kurbanları aracılığıyla çaldıkları hesap bilgilerini kullanarak kendi hesaplarına 55.000 dolardan fazla para aktarmışlar.

Günümüzün dijital baş belalarının bir diğer türüyse, gizlice sizi izlemekle görevlendirilen tuşa basmaları kaydedici (keystroke-logging) yazılımlar. Kendini İnternet ağları boyunca kopyalayan kötü niyetli bir saldırı amaçlı yazılımın bir parçası olarak bilgisayarınızın üzerine yerleştirilen bu yazılımlar, kurbanların bilgisayarında yazdığı her şeyi kaydetmek ve saldırganlara aktarmak için kullanılıyor. Kaydedilen bu bilgiler bilgisayarda bir metin dosyası üzerinde saklanıyor ve sanal dolandırıcı tarafından oluşturulmuş ücretsiz ve isimsiz bir e-posta hesabına

Nasıl Korunacağız?

İnternet üzerinden yapılan dolandırıcılıklar kendilerini sürekli geliştiriyor olduklarından, biz İnternet kullanıcılarının da her geçen gün daha dikkatli ve temkinli davranmamız gerekiyor. Kendimizi korumak için yapmamız gerekenlerin belli başlılarının bir listesi aşağıda yer alıyor. Bu listeyi uygulayıp hepimizin uygulaması, kendimizi korumamız için temel anahtar olabilir.

BİLGİSAYARINIZI TEMİZ TUTUN

Bilgisayarınızdaki koruma ve virüs tarama yazılımlarını sürekli güncelleyin. Bilgisayarınızda düzenli olarak virüs taraması yapın.

BİR ENGEL OLUŞTURUN

Windows işletim sisteminin içinde bulunan koruma duvarının aktifleştirildiğinden emin olun. Hatta en iyisi bir koruma duvarı yazılımı ya da kendi içinde koruma duvarı özelliği bulunduran bir yönlendirici satın alın.

KANDIRILMAYIN

Sizden kişisel ya da finansal bilgilerinizi isteyen tüm e-postalara karşı temkinli olun. Çünkü bankalar ve sanal mağazalar müşterilerine asla hesap bilgilerini güncellemelerini isteyen mesajlar göndermezler. Size ulaşan bir e-postanın doğruluğundan kuşku duyarsanız, hemen bu mesajı gönderdiği belirtilen şirketi arayın.

HERHANGİ BİR ŞEYE TIKLAMADAN ÖNCE DÜŞÜNÜN

E-posta tabanlı pek çok virüsün kendisini bilgisayarınıza kurması için tek bir tıklama yeterlidir. Ayrıca bir e-posta giriş yapmanız için belli bilgileri girmenizi gerektiren bir Web sitesini otomatik olarak açıyorsa mutlaka açılan bu pencereyi kapatıp o şirketin web sitesine URL adresini yazarak yeniden girmeyi deneyin.

KENDİ KENDİNİZE KONTROLLER YAPIN

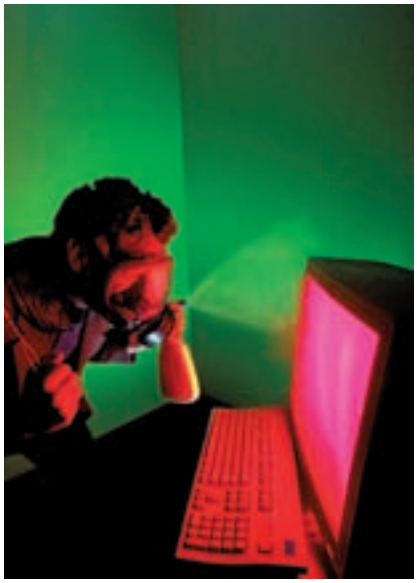
Banka hesabınızdaki ve kredi kartınızdaki hesap hareketlerini dikkatlice inceleyin. Soyguncular fark edilmelerini engellemek amacıyla sürekli olarak küçük miktarlarda aktarımlar yapacaklardır.

KAĞIT İZLERİNİZDEN KURTULUN

Kullanmadığınız kredi kartlarınızı ve kredi bilgilerinizi içeren kağıt halindeki bildirimlerinizi mutlaka yok edin.

ÇABUCAK HAREKETE GEÇİN

Kimlik bilgilerinizin çalındığını fark eder etmez hemen ilgili kurumu ve ülkenizdeki yetkili birimleri arayın.



düzenli bir şekilde e-posta olarak gönderiliyor. Sanal dolandırıcı da kendi e-posta hesabına gönderilen bu dosyaları sürekli inceleyerek kredi kartı numaralarını ve parolaları ele geçiriyor.

Eller Yukarı, Polis!

Sanal alemdeki dolandırıcılık suçlarının işlenme yöntemlerinin farklı olması, bu dünyadaki suçluları ele geçirmek için gereken yöntemleri de farklılaştırıyor. Sanal dolandırıcıları ele geçirmek isteyen yetkililerin, yapacakları baskınları saniye düzeyinde hassasiyetle ayarlamaları gerekiyor. Bu tür suçlarda "Eller yukarı, polis!" demek pek olası değil, çünkü yetkililer bunu diyene kadar suçlular klavyeleriyle birlikte çoktan kaçmış oluyorlar. Bu nedenle Kanada, Brezilya, Polonya, İsveç ve bir çok diğer ülkenin resmi yetkilileriyle birlikte çalışarak aylardır ShadowCrew isimli sanal suç sendikasını araştıran gizli servis ajanları siber gangsterlere arkadaşlarını uyarmak ya da suç unsuru taşıyacak kanıt niteliğindeki verileri bilgisayarlarından silmek için zaman vermemek için çok hızlı davranıyorlar. Bu sanal suç sendikasının web sitesi www. shadowcrew.com (şu anda kapatılmış durumda) sanal kimlik hırsızlığına yönelik bir tür sanal alışveriş sitesi gibi iş görüyor. Siber dolandırıcılar bu site üzerinden dünyanın her yerindeki kişilere ait kredi kartlarını, sosyal güvenlik numaralarını, vatandaşlık numaralarını ve anne kızlık soyadlarını kullanılmış araba parçaları gibi alıp satabiliyorlar. Son iki yıl içinde yaklaşık 4000 ShadowCrew üyesi, diğer insanların yaşamlarına ait 18 milyon e-posta hesabından ve buna bağlı kişisel ve finansal bilgilerden oluşan iki terabaytlık bilgi toplamışlar. 2004 yılının Ekim ayında düzenlenmiş baskınlarda tüm dünya genelinde bu sendikanın üyesi olan 28 şüpheli yakalanmış. Yetkililer baskın yaptıklarında, bu şüphelilerin çoğu klavyelerinin başında oturuyormuş. ABD uyruklu sanıkların altı tanesi 2005 yılının Kasım ayında kredi kartı ve banka hesaplarıyla ilgili yaptıkları dolandırıcılıklar konusunda suçlarını kabul etmişler. Bu ekibin verdiği zararın büyüklüğünü tam olarak belirlemek güç olsa da, yetkililere göre yüzlerce milyon dolar büyüklüğünde.

Neyse ki bir yandan teknolojiyle birlikte sanal dünyadaki suçlar gelişirken, tüm ülkelerdeki resmi kurumlar da bu konuyla ilgili yasal düzenlemeleri oluşturmak için çabalarını artırmakta. ABD'deki pek çok eyalet özel kişisel bilgilerin ve vatandaşlık numarası gibi bilgilerin belli resmi belgelerde, sürücü ehliyetlerinde ve benzer diğer resmi evraklarda tanımlayıcı olarak kullanılmasını kısıtlamak için gerekli çalışmalara başlamış durumda. Yasa düzenleyiciler ayrıca, İnternet üzerinden para transferi yapan her türlü kurumun veritabanlarını, korsanlarca bilgileri ele geçirilen müşterilerini haberdar edecek şekilde kurmalarını sağlamaya çalışıyorlar. Bankalar ve kredi kartı şirketleriyse, teknolojik altyapılarının kurulum aşamasından başlayarak, daha gelişkin koruma teknolojileri kullanmaya özen gösteriyorlar. Ama yine de bütünüyle güvenli bir İnternet ortamı olması için daha gidilecek uzun bir yol var. Bankaların ve e-ticaret sitelerinin kullanıcılarından aldıkları sorgulama bilgilerini ve korumaya yönelik teknolojik yatırımlarını artırmaları, devletlerin bu konuyla ilgili yasal düzenlemelere önem vermesi de kuşkusuz tek başına yeterli değil. Tüm dünya genelindeki İnternet kullanıcılarının da daha bilinçli olması ve temkinli davranması, bu tür dolandırıcılıkların sonuçsuz kalmasını sağlayacak en önemli etmenlerden biri.

Türkiye'de Durum

Türkiye'de de son yıllarda özellikle İnternet bankacılığı uygulamalarının kullanımının yaygınlaşmasıyla, İnternet üzerinden yapılan dolandırıcılıklar da gündeme gelmiş durumda. 2005 yılının Mayıs ayında bir bankanın İnternet sitesi üzerinden yapılan yaklaşık 74.000 YTL'lik soygun, gündeme bomba gibi düşmüştü. Bankanın asıl web adresine benzeyen bir sahte adrese, bankanın web sayfasının birebir kopyasını yerleştiren siber soyguncular, bu yolla çoğu kişinin kullanıcı bilgilerini ele geçirmişlerdi. Bu olayda mağdur olan kişilerin en büyük şikayetiyse, TC kanunlarının İnternet üzerinden işlenen bu tür suçlarla mücadelede son derece yetersiz olması. Mağdurların çoğu davalarının bir türlü sonuçlanmamasından, sonuçlanan davaların da mağduriyetlerini gidememiş olmasından ve temyize gitmek durumunda kalmış olmalarından ötürü hala kayıplarını giderebilmiş durumda değiller.

Ayşenur T. Akman

Kaynaklar:
Krebs, B.; "Do You Know Where Your Identity Is?", Popular Mechanics, Şubat 2006.
Yardımcı Kaynaklar
Knight, W.; "Thousands of Zombie PCs Created Daily", New Scientist, http://www.newscientist.com/article.ns?id=dn6420
http://www.antivirus.odtu.edu.tr/
http://www.sanalbankamagdurlari.com
http//turk.internet.com
http://project.honeynet.org
http://www.radikal.com.tr