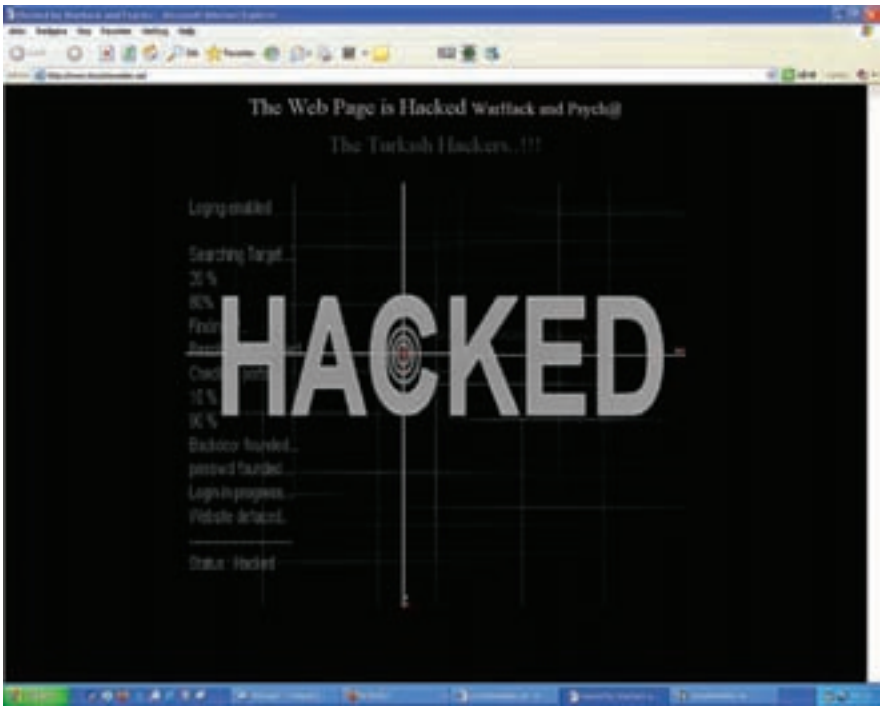
# BİLİŞİM KORSANLIĞI

Dünyada artık yedi kıta var. Yedinci kıta İnternet! Daha önce altı kıtaya yayılmış olan milyarlarca insan, bugün aynı zamanda sanal bir ortamda yaşıyor. Gerçek dünyadaki pek çok hizmet artık İnternet üzerinden de veriliyor. Aslında "yedinci kıta" tamamen teknoloji üzerine kurulu. Teknoloji geliştikçe de sanal yaşamın kalitesi artıyor. Bu kıtada ülke sınırları, kültürel farklılıklar, kurallar ve hukuk gerçek dünyadaki gibi değil. Ayrıca burası, bir anlamda bir "bilgi kasası". Teknolojiyi iyi bilen birtakım sanal kimlikler bu kıtada istedikleri gibi at koşturabiliyorlar. Sanki tren yollarının yapıldığı, dinamitin yeni yeni kullanılmaya başlandığı, henüz tam ülke olamadığı için hukuk sisteminin bulunmadığı, insanların kendilerini korumak için bellerinde silah taşıdıkları 1800'lerin Amerikası'ndan söz ediyoruz... Teknoloji silahını kuşanarak yedinci kıtada hukuksuzca dolaşan bilişim korsanları da bir anlamda 1800'lerin Amerikan kovboylarına benziyorlar...

Gün geçmiyor ki medyada bir bilişim korsanlığı haberi okumayalım. İnsanları e-posta yoluyla tuzağa düşürmek isteyenler, web sitesi çökertenler, şifre ele geçirip banka hesabından para çekenler ve başkasının bilgisayarına girip çıkanlar... Yani çok da savunulacak yanı olmayan işler. Öte yandan okuduğumuz haberlerden, bilişim korsanı olmanın bilişim teknolojilerini iyi bilmekle ve meraklı olmakla da bir ilgisi olduğunu anlıyoruz. Peki, bütün korsanları aynı sınıfa koyarak mı değerlendirmeliyiz? Bazı yorumcular, bilişim korsanlarını kendi içlerinde beyaz şapkalılar, siyah şapkalılar diye ikiye ayrıyor; tıpkı eski Amerikan filmlerindeki iyi ve kötü kovboylar gibi. Beyaz şapkalılar "yalnızca meraktan içeri girip bakacağım" diyerek bilgisayar sistemlerine sızıp, bir zarar vermeden çıkanlara; siyah şapkalılar da "teknoloji silahı" aracılığıyla çaldıkları şifrelerimizle banka hesabımızı boşaltan ya da bilgisayar sistemlerimizi kullanılamayacak hale getirenlere deniyor.



"Bilişim korsanı" teriminin İngilizce karşılığı olan hacker sözcüğü ilk kullanıldığı zamanlarda olumlu bir anlama sahipmiş. Hacker, 1960'larda ABD'de üniversite çevrelerinde bilgisayar donanımını kurcalamaktan hoşlananlara ya da bilgisayar yazılımlarını daha çabuk ve verimli çalışmaları için güncelleyen meraklılara deniyormuş. 1970'lerin başındaysa hacker sözcüğü, olumsuz bir anlam kazanarak, telefonla bedava konuşabilmek için telefon şirketini türlü numaralarla kandıranları anlatmak için kullanılmaya başlanmış. Hacker'lığın tarihi, Vietnam savaşı gazisi John Draper'ın, mısır gevreği kutusundan çıkan düdüğü üflediğinde telefonun çevir sinyali verdiğini fark etmesiyle başlıyor. Draper'ın bu yöntemi daha sonra ülke çapında yaygınlaşıyor. Bu yöntemi kullananlara da "hacker" deniyor. Teknolojinin gelişmesiyle hacker'ların ilgi alanları telefondan bilgisayara kayıyor.

Peki bilişim korsanları kendilerini nasıl tanımlıyor? Bazı bilişim korsanları, kendilerini teknolojiyi öğrenirken adrenalin salgılamayı seven meraklılar olarak tanımlıyor; bazılarıysa yalnızca meraklarının peşinden gittiklerini söylüyorlar. Öte yandan ülkelerin ya da gizli servislerin sanal dünyadaki hakimiyetlerine engel olmak için bir araya geldiklerini söyleyen bilişim korsanlarına rastlamak da olası. Bunun dışında kendilerini ülkelerinin koruyucusu ilan ederek, gündeme bağlı olarak düşman kabul ettikleri ülkelerin web sitelerine saldıranlar da var.

## Nasıl Saldırıyorlar?

Bilişim korsanlığının bilinen yüzlerce yöntemi var. Şimdi bellibaşlı birkaç tanesine göz atalım.

Bir siteye saldırarak onu çökertmek, belirli bir yöntem izlemeyi gerektirir. Bir bilişim korsanı, bir siteyi anında tümüyle çökertecek sihirli bir formüle sahip değil. Bilişim korsanının bir siteye saldırması için önce hedefini tanıması gerekir. Hedefi hakkında bilgi edinen korsan, daha sonra çeşitli yazılımlar yardımıyla hedefini "dinleyerek" sistemin güvenliğiyle, açıklarıyla ve kullanıcı hesaplarıyla ilgili bilgi sahibi olur. Ardından sistemde her şeyi yapmaya yetkili bir kullanıcı hesabı ele geçirir. Bundan sonra hedef sisteme rahatça girip çıkmak için bir "arka kapı" açar. Artık korsan, sistemin efendisi olmuştur ve yazılımlara istediği zararı verebilir... Bilişim korsanları saldırılarını genellikle hazır yazılımlar kullanarak yaparlar. İnternet'te bu amaca uygun binlerce bedava yazılım bulunabilir. Dolayısıyla bilişim korsanı olmak için her zaman bilgisayar alanında derin bilgiye sahip olmak gerekmiyor.

## Hedef Hakkında Bilgi Toplamak

Bir hırsız gireceği evde kimlerin yaşadığını, herhangi bir güvenlik sisteminin olup olmadığını, evde yaşayanların kapıları-pencereleri açık bırakıp bırakmadığını öğrenmek ister. Bir bilişim korsanı da tıpkı bir hırsız gibi, gireceği sistemin güvenlik bilgilerini elde etmeye çalışır. Bunun için öncelikle bilgi toplar. Bu konuda en değerli bilgi kaynakları İnternet, sistem kullanıcılarının basına verdiği bilgiler ve "sosyal mühendislik" taktikleridir. Arama motorlarını kullanarak bilgiye ulaşmak, bilişim korsanlarının en kolay bilgi toplama yollarından biridir.

Bilişim korsanları, "Leet yazım biçimi" denen bir yazım biçimini sık kullanırlar. Leet yazım biçimi, sözcüklerin İnternet, oyun ve chat kullanıcıları tarafından değişikliğe uğratılmış hallerinden oluşuyor. Örneğin, Leet yazım biçiminde, hacker sözcüğü "h4x0r" olarak yazılır. Bilişim korsanları, bu yazım biçimini kullanmayı hem eğlenceli hem de "elit" buluyorlar. Google arama motorunun, Leet yazım biçiminde arama yapmayı kolaylaştıran bir sayfası var (http://www.google.com/intl/xx-hacker/).

Google'da bazı operatör sözcüklerin (intitle, inurl, intext, source gibi İngilizce sözcükler) yardımıyla yapılabilen gelişmiş arama yöntemleri ve aynı anda onlarca arama motorundan sonuç getirebilen çeşitli yazılımlar da, yine bilişim korsanlarının bilgi toplarken işlerini kolaylaştırıyor. (Operatör sözcüklerle arama yöntemleri için http://www.google-guide.com/advanced_operators_1.html adresine bakılabilir.) Ayrıca İnternet'te tutulan çeşitli kayıtlar da korsanın bilgi dağarcığının büyümesini sağlıyor. Örneğin, www.archive.org adresinden, bir sitenin eski sayfalarını görmek olası.

İnternet'te herhangi bir sitenin tüm kimlik bilgileri (sitenin sahibi, site sahibinin iletişim bilgileri vb) çeşitli veritabanlarında tutuluyor. Bunlardan biri, "Whois Veritabanları". http://www.who.is/ ve http://www.dotdir.com/ adreslerine girerek bir web sitesinin kimlik bilgilerine ulaşılabiliyor.


Bilişim korsanının bilgi toplama yollarından biri de, hedef siteyle ilgili olarak medyada ya da İnternet'te çıkan haberler. Özellikle bilgi teknolojileriyle ilgili dergilerde sık rastladığımız, "A şirketi alt yapısını değiştirerek X işletim sistemine geçti" ya da "B şirketi alt yapısını X yönlendiricileriyle donattı" gibi haberler bilişim korsanı için önemlidir. Çünkü saldırı sırasında kullanılacak yazılımlar, kurbanın bilgisayarının işletim sistemine ve ağ yapısına göre değişiklikler gösterir.

Başka bir bilgi toplama yöntemi de "sosyal mühendislik". Bedava telefon etmek için telefon şirketlerini çeşitli yollarla kandıran ve daha sonra kredi kartı numarası çalmak suçundan tutuklanıp hapse giren en ünlü bilişim korsanlarından biri olan Kevin D. Mitnick, "Aldatma Sanatı" adlı kitabında bu yöntemi tüm ayrıntılarıyla anlatır. Bu yöntemde korsan, bazen yalan söyleyerek, bazen acındırarak, bazen korkutarak, bazen yardım isteyerek, bazen de yardım etme teklifinde bulunarak karşısındaki kişiyi kandırır ve ağzından bilgi alır (kullanıcı adı, şifre, bilgisayar adı gibi).

Ağ üzerinde bulunan bir bilgisayarla iletişim kurulup kurulamayacağını anlamak için "ping" denilen bir komut kullanılır. Böylece başka bir bilgisayarın iletişime hazır olup olmadığı kolayca öğrenilebilir. Bu, tıpkı birinin karşısındaki insana "Bir dakika dinler misiniz?" sorusuna, karşısındaki kişinin "Buyrun, sizi dinlemeye hazırım!" diyerek yanıt vermesine benzer. Ping komutu çalıştırıldığında, hedef bilgisayara "yankı isteği mesajları" gönderilir. Hedef bilgisayar çalışır durumdaysa buna, "iletişime uygunum" anlamında bir yanıt mesajı verir. Bilişim korsanı, saldıracağı bilgisayarın açık ve iletişime hazır olup olmadığını anlamak için ping komutunu çalıştırır.

## Bir Gece Ansızın Gelebilirim

"Port (giriş kapısı)", bir bilgisayarın aynı anda birden fazla uygulamayı çalıştırmasını sağlayan bir numaradır. Bu numara, bilgisayara hangi yazılımı çalıştırması gerektiğini anlatır. Bilişim korsanı, port taraması yaparak açık port bulmaya çalışır. Güvenlik duvarıyla korunmayan bir port bulursa çeşitli yanıltma yöntemlerini kullanarak bu bilgisayara erişebilir.

Port taramaları, en sık TCP (Transmission Control Protocol: İletim Denetimi Protokolü) üzerinden yapılır. TCP, iki bilgisayarın web siteleri yoluyla bağlantı kurmasında kullanılan gü-

venli iletişim kuralları bütünüdür. TCP'nin güvenilirliği, bilgisayarlar arasında iletişim kurulurken "üç adımda uzlaşma" (three way handshaking) diye bilinen yöntemi kullanmasından kaynaklanır. "Üç adımda uzlaşma" yöntemini açıklamak için şöyle bir örnek verebiliriz: Bir X bilgisayarının, Y sunucusunda bulunan web sitesiyle bağlantı kurmak istediğini düşünelim. X bilgisayarının İnternet tarayıcısına Y sunucusunun web adresi yazılıp "enter" tuşuna basıldığında "üç adımda uzlaşma" süreci başlar. Önce X bilgisa-

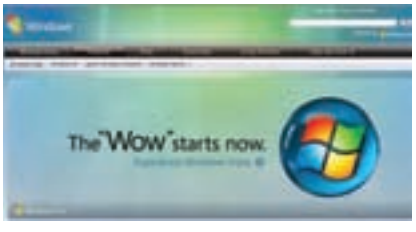
yarı, Y web sunucusuna, bağlantı kurmak istediğini gösteren bir mesaj yollar (1. mesaj). Gönderilen bu mesajı alan Y sunucusu, X bilgisayarından gelen mesajı aldığına ilişkin bir karşı mesaj gönderir (2. mesaj). X bilgisayarı, Y sunucusunun yanıt mesajını aldığına ilişkin yeni bir onay mesajını (3. mesaj) Y sunucusuna gönderir ve iki bilgisayar arasında veri alışverişi başlar. Bu süreç içinde mesajlarla birlikte verilerin sıra numaraları da gönderilir.

Web sunucusundan bilgi almak için çeşitli port tarama yöntemleri vardır. Kolay olması nedeniyle çaylak bilişim korsanlarının kullandığı "TCP Connect" taramasında hedef sunucunun portlarına yukarıda sözünü ettiğimiz 1. mesaj gönderilir. Buna yanıt olarak 2. mesaj gelirse bilişim korsanı sunucunun "üç adımda uzlaşma"ya hazır olduğunu anlar. Öte yandan sunucunun bir güvenlik duvarı (firewall) varsa 2. mesaja yanıt olarak "1. mesajı yeniden

gönder” mesajı iletebilir. Bu durumda korsan, hedef sunucunun güvenlik duvarı olduğunu anlar. Başka bir port tarama yöntemi de “üç adımda uzlaşma” sürecinde hedef sunucuya “1. mesajı yeniden gönder” mesajları iletmektir. İki bilgisayar arasındaki bağlantının sonlanacağını gösteren “bitti” mesajı da diğer bir port tarama yöntemidir. Günümüzde çoğu güvenlik duvarı port taramalarını saptayabilir.

## Bana İşletim Sistemini Söyle, Sana Kim Olduğumu Göstereyim

İşletim sistemlerinin ilk sürümleri pek çok güvenlik açığına sahiptir. Bu güvenlik açıkları İnternet’teki çeşitli sitelerde ilan edilir. Güvenlik açıklarını kullanan yazılımlar sayesinde bilgisayarlardaki kullanıcı hesapları ve paylaşım bilgileri görülebilir. Bir bilgisayarın işletim sisteminin ne olduğunu öğrenmek için ona, “üç adımda uzlaşma” mesajları gönderilir. Bu mesajlara gelen ya da gelmeyen yanıtlar, işletim sisteminin ne olduğunu belli eder. Çünkü işletim sistemleri bu mesajlara farklı yanıtlar verir. Ağ trafiğini izlemek, ftp ve telnet gibi uygulamalarla bağlantı kurmak da işletim sistemiyle ilgili bilgi sağlar.




İşletim sisteminin ne olduğunu bulan bilişim korsanı, bundan sonra bilgisayardaki kullanıcı hesaplarını ve paylaşımları görmeye çalışır. Korsan, çeşitli komutlar ya da bu işi yapan yazılımlar yardımıyla aradığı bilgilere kısa zamanda ulaşabilir. İşletim sisteminin belirlenmesini önlemenin yollarından biri, bilgisayarın kullanılmayan portlarını kapatmak ve sistem açıklarını kapatan yazılımları (yamalar) yüklemek. Saldırıları saptayan sistemler kurmak ve yedekleme yapmayı da asla unutmamak, alınabilecek diğer önlemlerden.

## Bilişim Korsanının Gözü, Kulağı: Sniffer Yazılımları

George Orwell “1984” adlı romanında, bir “Büyük Birader”in insanları her yerde gözleyeceği kestiriminde bulunmuştu. Günümüzde bilişim korsanlarının ağ trafiğini “sniffer (koklayıcı)” adlı yazılımlarla izlemesi, insana, Orwell’in kestiriminin en azından sanal ortamda bir oranda gerçekleştiğini düşündürüyor. Aradaki fark, sanal ortamdaki birader sayısının çokluğu!.. Sniffer yazılımlarının ağ gözlemek dışında gidip gelen veriler yakalayabilme özelliği de var ve bunların incelenmesiyle çok özel bilgilere ulaşmak olası.

Sniffer yazılımlar, ağ oluşturmak için kullanılan “hub” adı verilen cihazların özelliklerinden yararlanarak bilgi toplarlar. Hub’lar, bir bilgisayardan gelen bilgiyi kendilerine bağlı tüm bilgisayarlara gönderirler. Sniffer yazılımlar, hub’ların gönderdiği veri paketlerini yakalarlar. Verileri, hub’lara göre daha verimli ve güvenli bir şekilde aktaran “yönlendirici (router)” cihazların bulunduğu ağlar da sniffer yazılımlarla “dinlenebilir”. Sniffer yazılımlar, bir bilgisayarı ağa bağlayan kart numaralarını ele geçirebilir; yönlendirici cihazlardaki bazı bilgi tablolarında değişiklikler yapabilir; başka bilgisayara gidecek veri paketlerinin bulundukları bilgisayara gelmesini sağlayabilirler.

## İnternet’ten Alışveriş Yaparken...

Bilişim korsanlarının, İnternet’te alışveriş yapanların bilgilerini elde etmesinin bir yolu da DNS sorgulamalarında kurban kullanıcının bilgisayarını kandırma yoluna başvurmaktır. DNS, (Domain Name System: Alan Adı Sistemi) İnternet tarayıcısına yazdığımız adreslerin (alan adlarının) karşılık geldiği “İnternet Protokol (IP)” numaralarını tutan bir İnternet servisidir. DNS servisi, bir web sitesine IP numarası yazarak bağlanma zorluğundan bizi kurtarır. Böylece İnternet adreslerini kolaylıkla aklımızda tutarız. DNS sorgusu da, İnternet tarayıcımıza ilk kez yazdığımız bir adresin hangi IP numarasına karşı geldiğinin anlaşılması için DNS bilgilerini tutan veritabanlarından bilgi çekme yoludur. DNS sorgulaması yapılırken aldatma yönteminde, bilişim korsanı kendine bir web sitesine ilk kez giriş yapan bir kurban seçer. Çünkü bu aldatma yönteminin başarısı, kurbanın bilgisayarının DNS sorgusu yapmasına bağlıdır. Kurbanın bilgisayarının DNS sorgusu yapması da sniffer türü bir yazılımla ağ gözlenerek anlaşılabilir. Korsan, kurbanın bilgisayarı DNS sorgusu yaptığında, DNS servislerinden gelen “girilen adresin IP numarası şudur..” şeklindeki yanıtı yakalayarak değiştirir ve hedef web sitesinin IP’si yerine kendi IP numarasını yazarak kurban kullanıcıya yollar. Korsanın kullandığı yazılımlar, kurban kullanıcının hedef web sitesine korsanın bilgisayarı üzerinden bağlanmasını sağlar. Böylece kurban kullanıcının hedef web sitesine girdiği her bilgi (kullanıcı adı, şifreler, banka hesap numarası gibi) önce korsanın bilgisayarına ulaşır, ondan sonra hedef web sitesine gider... Ancak bu işlemler sırasında kurban

kullanıcının bir kurtulma şansı vardır. Kurban kullanıcı, korsanın bilgisayarının hedef web sitesine bağlanmadan önce kendisinin bilgisayarına gönderdiği sahte güvenlik sertifikasıyla ilgili uyarı mesajını dikkate alırsa ve hedef web sitesine girmekten vazgeçerse bu oyundan kurtulur. Yok eğer kurban kullanıcı, bu uyarıda yer alan ve bağlanılacak sitenin güvenliğinin olmadığına ilişkin notu dikkate almayıp "yes" tuşuna basarsa bilişim korsanının tuzağına düşer.

## Oturum Ele Geçirme

TCP oturumlarının ele geçirilmesi başka bir bilişim korsanı aldatmacası. TCP'nin iki bilgisayar arasında ilişki kurulurken yalnızca bir kez güvenlik denetimi yapması, buradaki aldatmacaya zemin hazırlıyor. Bu yöntemde, iki bilgisayar arasındaki üç adımda uzlaşma süreci bilişim korsanı tarafından kötüye kullanılır. Daha önce de sözünü ettiğimiz gibi, "üç adımda uzlaşma"da bilgisayarlar birbirlerine çeşitli mesajlar ve sıra numaraları gönderir. Sıra numaraları, gelen veri paketlerinin doğru sırada okunmasını sağlar. Böylece bir karışıklık durumunda bilgisayara hangi verinin gitmediği kolayca saptanır. Eğer bir korsan, bir web sunucusuyla başka bir kullanıcı arasındaki bağlantıda kullanılan sıra numarasını doğru tahmin ederse, sanki iletişim talebini kendi yapmış gibi hedef sunucuya bağlanabilir. Bunu gerçekleştirmek için bilişim korsanının kendine, girmek istediği sunucuya ftp ya da telnet gibi bir uygulamayla bağlanan bir kurban kullanıcı bulması gerekir.

Böyle bir durumda bilişim korsanı, bir sniffer yazılımıyla ağı gözleyerek, ftp'yi ya da telnet'i çalıştıran bir kullanıcı ortaya çıkana kadar bekler. Sabırla koruk nasıl üzüm olursa, bilişim korsanının da beklediği bir gün gerçekleşir ve kurban kullanıcı, korsanın girmeyi hedeflediği sunucuya ftp'yle bağlandığında işlem başlar. Korsan, hedef sunucuyla kurbanın bilgisayarı arasında alınıp verilen verileri ve sıra numaralarını bir sniffer yazılımıyla yakalar. Sonra kurbanın bilgisayarına, hedef sunucuya bağlanmasına engel olmak amacıyla çok miktarda bozuk veri paketi gönderir. Bu bozuk veri paketi saldırısı karşısında kurbanın bilgisayarı devre dışı kalır. Korsan, kurbanın IP numarasını da kullanarak, hedef sunucunun, kurbanın bilgisayarından beklediği sıra numarasını (sanki kurbanın bilgisayarı gönderiyormuş gibi) gönderir. Daha sonra da korsan, kurban kullanıcı tarafından açılmış oturumu kendi bilgisayarı üzerine alarak hedef web sunucusuna girer...

## Zombi Saldırıları

Bilişim korsanlarının verdikleri zararlardan biri de bir bilgisayarı devre dışı bırakmak ya da kaynaklarını tüketerek çökertmektir. DoS (Denial of Service: hizmet aksatma) adı verilen bu saldırılarda, bilişim korsanı hedef sunucuya çok sayıda bozuk veri paketi göndererek işletim sisteminin kilitlenmesine ya da çökmesine yol açar. Kaynakların tüketilmesine yönelik saldırılarda da sunucu, bilgisayara çeşitli yollarla gönderilmiş kaynak emici yazılımların çalıştırılması yoluyla çökertilir. DoS saldırılarının birden fazla bilgisayarla yapılanına "DDoS saldırısı" denir. Bilişim korsanının kendisinin yazıp bilgisayarlara yüklediği zombi yazılımlar (e-postaya ekli gelen yazılımların çalıştırılmasıyla bilgisayara yüklenen ya da doğrudan korsanın bilgisayarlara gizlice yaptığı yüklemeler) saldırı anı geldiğinde hep birlikte hedef sunucuya bozuk veri paketi göndererek onu çökertirler.


## "1. Mesaj" Bombardımanı

Bu tür saldırılarda hedef sunucuya "üç adımda uzlaşma"daki 1. mesajdan çok sayıda gönderilir. Sunucu gelen mesajlara 2. mesajla yanıt verir. Ancak sunucunun gönderdiği veri paketleri bilişim korsanına ulaşmaz; çünkü korsan IP numarasını gizlemiştir. Sunucu, kendisiyle sözde iletişim kurmak isteyen bilgisayardan gelen mesaj bilgilerini belleğine kaydeder; ancak pek büyük olmayan bellek alanı gelen binlerce istek karşısında kısa sürede dolar ve sunucu, ilgili portu kapatarak iletişimi durdurur.

## Güvenli Şifreniz Yoksa!..

Bir bilgisayar sisteminin kullanıcı adlarını ele geçiren korsanın önüne çıkan engellerden biri, kullanıcı şifreleridir. Bir korsan, güvenli şifre oluşturma kurallarına uymayan şifreleri, şifre kırma yazılımlarıyla çok kısa süre içinde kırabilir. Bu tür yazılımlar şifreleri, bi-

## Bilişim Korsanlığı Bir Suç!

**Güvenlik birimlerindeki uzmanlara göre bilişim korsanının iyisi kötüsü yok. Uzmanlar, ister beyaz şapkalı olsun ister siyah şapkalı, bir bilgisayar sistemine izinsiz giren kişinin suç işlediğini söylüyorlar. Dolayısıyla güvenlik birimlerinin bu kişilere karşı yasada belirtilen süreci işletmekle görevli olduklarını hatırlatıyorlar. Öte yandan günümüzde, izinsiz girilen bilgisayarların başka ülkelerde olmasının, suçun izlenemezlik yüzünden araştırılmasına engel olmadığını da belirten uzmanlar, çocuk pornosuyla uğraşanların yakalanması konusundaki uluslararası işbirliğine ve kimi ülkelerle yapılmış ikili suçlu iadesi anlaşmalarına dikkati çekiyorlar... Peki ülkemizde yakalanmış bilişim korsanı var mı? Evet, varmış!.. En son üniversiteli bir genç, bir gazetenin web sitesine saldırdığı için yakalanıp hüküm giymiş... Güvenlik birimlerindeki uzmanlar, bilişim korsanlarıyla mücadele etmek için, bilgiişlem merkezlerinde yalnızca güvenlikten sorumlu personellerin istihdam edilmesini öneriyorlar.**

**"Suçluyu kazı, altından insan çıkar" düşüncesinden hareketle psikiyatrist Doç. Dr. Külteğin Ögel'e bilişim korsanları hakkındaki görüşünü sorduk. Ögel, bilişim korsanlığı suçu işlemenin dürtüsel yanı üzerinde durarak, tıpkı kumar bağımlıları gibi, bazı bilişim korsanlarının da kendilerini başkasının bilgisayarıyla ilgilenmekten alıkoyamadıklarını belirtti. Ya da şifre görünce dayanamayıp onu çözmeye çalışan bilişim korsanlarının olduğunu söyledi. Öte yandan Ögel, bilişim korsanlarında empati eksikliği bulunduğunu belirterek, topluma ya da insanlara zarar verebilen, yaptıklarından pişmanlık duymayan ve kendilerini hep haklı gören bir tutum sergilediklerini anlattı. Ögel, bilişim korsanlarının "ülkeyi savunma" düşüncesiyle yaptıkları eylemlerin topluma iyi bir durum gibi yansıtılmasının, onları bu olumsuz davranışlarını sürdürme konusunda kışkırttığını da belirtti.**

lindik şifreler, veritabanındaki kayıtlarla karşılaştırarak ya da her bir karakteri deneme yanılma yöntemiyle bularak çözerler. İçinde yalnızca adlar, tarihler ya da sayılar bulunan bir şifre, sözü edilen yöntemlerin ortak kullanılmasıyla çok kısa bir zaman dilimi içinde çözülebilir. Ancak güvenli şifre üretme kurallarına uygun şifreler bazen yıllar boyu üzerinde çalışılsa da çözülmezler. Güvenli şifre oluşturmayla ilgili pek çok kaynağa İnternet üzerinden ulaşılabilir.

## Bu Çerez Başka Çerez

Çerezler (cookie) bir web bağlantısı sırasında sunucuyla kullanıcının birbirlerini tanımaları için tutulan kayıtlardır. Hem web sitesinde hem de kullanıcının bilgisayarında bulunurlar. Web sitelerine bağlanırken kullanıcı adını yazar yazmaz karşımıza hazır olarak çıkan şifre bilgilerimiz, çerez kayıtlarının bulunduğu metin dosyalarından gelir. Kullanıcı adı ve şifre bilgilerinin çoğu kez şifrelenmemiş olarak bulunması, çerez dosyalarının zayıf yanıdır. Sniffer yazılımlarıyla ağı dinleyen bir bilişim korsanı, yakaladığı verilerin içinde bulunan çerez dosyalarına özel ilgi(!) gösterir. Çerez saldırılarından korunmanın en iyi yolu işletim sistemlerinin gönderdiği yama yazılımları bilgisayara yüklemek ya da İnternet tarayıcınızın güvenlik önlemlerini uygulamaktır.

## Hata Mesajlarından Bilgi Öğrenme

Bilişim korsanları, web servislerindeki veritabanlarından bilgi çekmek için bile bile hatalı sorgulama cümlecikleri gönderirler. Bu cümlecikler, veritabanlarından hangi bilginin istendiğini belirtir. Web servisinde bulunan veritabanları bu tür sorgulamalara hata mesajıyla yanıt verirler. Hata mesajının içinde veritabanıyla ilgili bazı doğru bilgiler de bulunur. Korsan, her yanlış sorgu için veritabanınından gelen hata mesajının içinde bulunan doğru bilgileri biriktirerek sistem hakkında yeni bilgilere ulaşır. Eğer sistem yöneticisi veritabanı sorgularına bazı kısıtlamalar getirmezse, korsan, veritabanlarında tutulan önemli bilgilere ulaşabilir. Bu aldatma türüne "SQL Injection" deniyor...

## Oltayla "Şifre" Tutmak

Genellikle kendini banka gibi kuruluşlardan geliyormuş gibi gösteren e-postalar, bilişim korsanlarının sevdiği "özel bilgi" elde etme yöntemlerinden biri. Bu yöntemde korsan, herkese içinde bir İnternet bağlantısı ve banka yetkilisinden gelen, "lütfen X bankasındaki bilgilerinizi güncelleyiniz" içe-


rikli bir açıklamanın bulunduğu e-postalar gönderir. İnternet bağlantısı tıklandığında da korsanın daha önceden hazırladığı bir kimlik bilgileri kayıt sayfası açılır. Buraya kaydedilen her özel bilgi, bilişim korsanına gider. Bu yöntem için, İngilizce password (şifre) ve fishing (balıkçılık) sözcüklerinden türetilmiş olan ve oltayla "şifre" yakalamayı ifade eden "phishing" sözcüğü kullanılır.

## Trojanlar

Trojan, Türkçe'de "Truvalı" anlamına geliyor. Trojan adı verilen yazılımlar, antik dönemde Truva atının yaptığının bir benzerini yapıyor; yani bilgisayarın kapısını bilişim korsanına açıyor. Trojanlar, aslında uzaktaki bilgisayarı yönetmeye yarayan yazılımlar. Genellikle korsanın gönderdiği e-postaya ekli yazılımın çalıştırılmasıyla bilgisayarlara bulaşıyorlar. Bulaşınca da uzaktaki korsanın bilgisayarına kullanıcı ve şifre bilgilerini, basılan bütün tuşların

kayıtlarını gönderebiliyorlar. Bu tür yazılımlara, bilişim korsanının kurban bilgisayara rahatlıkla giriş yapmasını sağladığı için "back door (arka kapı)" yazılımları da deniyor. Bilgisayarda anti-virüs yazılımı bulundurmak ve gelen e-postaların içindeki bilinmedik dosyaları çalıştırmamak, alınabilecek önlemlerin bazıları.

## "Korsansavar" Önlemler

Bu konuda söylenecek pek çok söz olmakla birlikte korsanları uzak tutacak bazı önlemler şöyle sıralanabilir: Düzenli yedek almak, bilgisayarda güvenlik duvarı ve anti-virüs yazılımları bulundurmak, işletim sistemi yamalarını yüklemeyi unutmamak, içinde dosyalar bulunan, göndereni belirsiz e-postaları silmek, güvenlik sertifikasıyla ilgili mesaj pencerelerini ciddiye almak, yeni bir yönetici hesabı oluşturarak işlemler sırasında yalnızca bu hesabı kullanmak, gereksiz yere sistemde kullanıcı hesabı açmamak, kullanılmayan portları kapatmak, şifreleri güvenlik kurallarına göre oluşturmak, bilgisayarınızı kullanmadığınız zaman açık tutmamak, acil bir durum planı hazırlamak, bilgisayar günlüklerini (log dosyalarını) kullanmayı öğrenmek...

Koray Özer


**Kaynaklar**

Yılmaz, Davut, Hacking,Bilişim Korsanlığı,Hayat, İstanbul,2005.
Dirican, Can Okan, TCP/IP ve Ağ Güvenliği, Açık Akademi, İstanbul, 2005
Mitnick, D.Kevin ve Simon, L.Simon , Aldatma Sanatı, Ankara,2005.
http://www.howstuffworks.com/web-server.htm
http://www.windowsecurity.com/articles/Common_Attacks.html